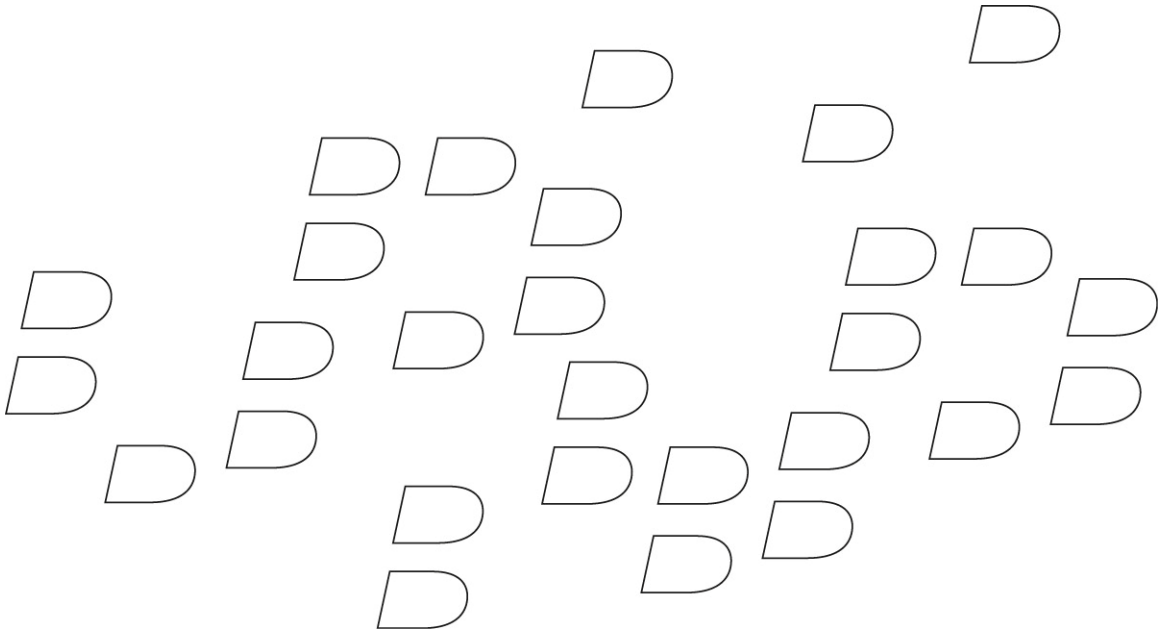


BlackBerry Enterprise Solution

Security Technical Overview

for BlackBerry Enterprise Server Version 4.1 Service Pack 5 and BlackBerry Device Software Version 4.5

© 2008 Research In Motion Limited. All rights reserved.

Contents

Wireless security 6
BlackBerry Enterprise Solution security 6
BlackBerry Enterprise Solution security features 7
New security features 8
BlackBerry encryption keys 9
Master encryption keys 9
Message keys 12
Content protection keys 14
Grand master keys 15
BlackBerry symmetric key encryption algorithms 15
Standard BlackBerry message encryption 17
Permitting third-party applications to encode BlackBerry device data 18
BlackBerry wireless messaging security 18
Receiving an email message on the BlackBerry device 18
Sending an email message from the BlackBerry device 19
Message attachment viewing security features 19
PIN-to-PIN messaging 20
Text messaging 21
Controlling unsecured messaging 21
Extending BlackBerry device messaging security 22
PGP Support Package for BlackBerry devices 22
PGP encryption 23
S/MIME Support Package for BlackBerry devices 24
S/MIME encryption 24
Decrypting and reading messages on the BlackBerry device using Lotus Notes API 7.0 26
Protecting stored data 27
Protecting stored messages on the messaging server 27
IT policy signing and storage on the BlackBerry device 28
Application password encryption and storage on the BlackBerry device 28
Protected storage of external memory on the BlackBerry device 28
Protected storage of user data on a locked BlackBerry device 29
Protected storage of master encryption keys on a locked BlackBerry device 31
Protected storage of master encryption keys on a BlackBerry device during a reset 31
Clearing the BlackBerry device memory 31

© 2008 Research In Motion Limited. All rights reserved.

BlackBerry architecture component security 33
BlackBerry Infrastructure 33
BlackBerry Enterprise Server 34
Messaging server 34
BlackBerry Configuration Database 34
BlackBerry MDS Services databases 36
Protecting the BlackBerry Enterprise Solution connections 37
SRP authentication 37
How the BlackBerry Enterprise Server and the BlackBerry Infrastructure handle undeliverable messages 38
BlackBerry Router protocol authentication 39
Authentication during wireless enterprise activation 40
TCP/IP connection 41
Messaging server to computer email application connection 42
Connections between the BlackBerry Desktop Manager and its components 42
BlackBerry MDS connections 43
Using two-factor authentication to protect connections to enterprise Wi-Fi networks 45
How the BlackBerry Enterprise Solution authenticates requests for wireless software upgrades 45
WAP gateway connections 46
Instant messaging server connections 46
Using segmented network architecture to prevent the spread of malware on your organization's network 46
Protecting Wi-Fi connections to the BlackBerry Enterprise Solution 47
Enterprise Wi-Fi network solution architecture security features 47
Accessing the BlackBerry Infrastructure 48
Supported security features of Wi-Fi enabled BlackBerry devices 48
IEEE 802.1X environment components 49
How the IEEE 802.1x environment controls access to the enterprise Wi-Fi network 49
Administering enterprise Wi-Fi network solution security using IT policy rules 50
Requiring protected connections to enterprise Wi-Fi networks 50
Using VPNs to protect connections to enterprise Wi-Fi networks 52
Using enterprise captive portals to protect connections to enterprise Wi-Fi networks or Wi-Fi hotspots 52
Authenticating a BlackBerry device user 53
Authenticating a user to a BlackBerry device using a password 53
Authenticating a BlackBerry device user using a smart card 53
Controlling BlackBerry devices 55

© 2008 Research In Motion Limited. All rights reserved.

Controlling BlackBerry device behavior using IT policy rules 55
Enforcing BlackBerry device and BlackBerry Desktop Software security 56
Controlling BlackBerry device access to the BlackBerry Enterprise Server 56
Controlling wireless software upgrades using the BlackBerry Enterprise Server 57
Protecting Bluetooth connections on BlackBerry devices 57
Controlling location-based services on the BlackBerry device 58
How the BlackBerry device protects its operating system and the BlackBerry Device Software 59
Protecting the BlackBerry device against malware 59
Protecting lost, stolen, or replaced BlackBerry devices 61
Remotely resetting the password of a content protected BlackBerry device 62
Remotely erasing data from BlackBerry device memory and making the BlackBerry device unavailable 62
Remotely resetting a BlackBerry device to factory default settings 63
Erasing all data and applications from the BlackBerry device memory over a physical connection 63
Unbinding the smart card from the BlackBerry device 64
Related resources 65
Appendix A: RIM Crypto API Interface 68
Cryptographic functionality that the RIM Crypto API provides 68
Appendix B: TLS and WTLS standards that the RIM Crypto API supports 71
Key establishment algorithm cipher suites that the RIM Crypto API supports 71
Symmetric algorithms that the RIM Crypto API supports 72
Hash algorithms that the RIM Crypto API supports 72
Appendix C: Previous version of wired master encryption key generation 73
Previous version of wired master encryption key generation process 73
Appendix D: BlackBerry device wipe process 74
Appendix E: Ephemeral AES encryption key derivation process 76
Appendix F: Power and electromagnetic side-channel attacks and countermeasures 77
Masking operation process that the AES implementation uses when content protection is turned on 77
Masking operation process that the AES implementation uses when content protection is turned off 77
Appendix G: BlackBerry Router protocol 79
How the BlackBerry Router protocol uses the Schnorr identification scheme 79
Examples of attacks that the BlackBerry Router protocol is designed to prevent 79
Process flow: Using the BlackBerry Router protocol to open an authenticated connection 80
Process flow: Using the BlackBerry Router protocol to close an authenticated connection 81
Appendix H: Enterprise Wi-Fi security methods that the BlackBerry device supports 82
EAP authentication methods that the BlackBerry device supports 82

© 2008 Research In Motion Limited. All rights reserved.

Encryption algorithms that the BlackBerry device supports for use with layer 2 security methods ... 83
EAP authentication methods and encryption algorithms with which the BlackBerry device supports the use of CCKM ... 84
VPN solution on the Wi-Fi enabled BlackBerry device ... 85
Appendix I: Algorithm suites that the BlackBerry device supports for negotiating SSL connections ... 85
Appendix J: RSA SecurID software token tokencode generation process ... 87
Appendix K: Content protection initialization process ... 87
Appendix L: Protocol for resetting the password on a content-protected BlackBerry device remotely ... 88
Cryptosystem parameters ... 88
Protocol process ... 89

© 2008 Research In Motion Limited. All rights reserved.

This document describes the security features of the BlackBerry® Enterprise Solution and provides an overview of the BlackBerry security architecture.

This document describes the security features that the BlackBerry® Enterprise Server Version 4.1 SP5, BlackBerry® Desktop Software Version 4.5, and BlackBerry® Device Software Version 4.5 support, unless otherwise stated. To determine if a feature is supported in an earlier software version, see the documentation for earlier versions of the BlackBerry Enterprise Server, the BlackBerry Desktop Software, and the BlackBerry Device Software.

For the full terms substituted by the acronyms in this document, see the *BlackBerry Enterprise Solution Security Acronym Glossary*.

Wireless security

Many enterprise organizations realize significant return on investments and productivity gains by extending access to their enterprise information to mobile employees. With an increased demand for mobile content and the threat of information theft, organizations have concerns about addressing security needs and requirements when evaluating wireless solutions. Without an effective security model, your organization might expose sensitive data, with financial and legal implications.

Powerful personal devices such as mobile phones and personal digital assistants can access and store sensitive data. Controlling access to these devices is an important issue. Leaving devices with remote access to sensitive data accessible to potentially malicious users might be dangerous.

The BlackBerry Enterprise Solution (consisting of a BlackBerry device, BlackBerry Device Software, BlackBerry Desktop Software, and the BlackBerry Enterprise Server) is designed to protect your organization from data loss or alteration in the event of

- malicious interception of data on your organization's network, while a BlackBerry device user is sending and receiving messages and accessing your organization's data over the wireless network using the BlackBerry device
- an attack intended to steal your organization's data, using malicious application code (for example, a virus)
- theft of the BlackBerry device

BlackBerry Enterprise Solution security

The BlackBerry Enterprise Solution implementation of *symmetric key cryptography* is designed to provide confidentiality, integrity, and authenticity implicitly.

Concept	Description	BlackBerry Enterprise Solution implementation
confidentiality	permits only the intended message recipient to view the contents of a message	Use encryption, which is data scrambling based on a secret key, to make sure that only the intended recipient can view the contents of the message.
integrity	enables a message recipient to detect if a third party altered the message data in transit between the message sender and the message recipient	• Protect each message that the BlackBerry device sends with one or more message keys comprised of random information, which is designed to prevent third-party decryption or alteration of the message data. • Enable only the BlackBerry Enterprise Server and the BlackBerry device to know the value of the master encryption key, recognize the format of the decrypted and decompressed message, and automatically reject a message either one receives that is encrypted with the wrong master encryption key and therefore does not produce the required message format upon decryption.

Concept	Description	BlackBerry Enterprise Solution implementation
authenticity	enables the message recipient to identify and trust the identity of the message sender	Require that the BlackBerry device authenticate itself to the BlackBerry Enterprise Server to prove that it knows the master encryption key before the BlackBerry Enterprise Server can send data to the BlackBerry device.

The BlackBerry Enterprise Solution is designed so that data remains encrypted (in other words, it is not decrypted) at all points between the BlackBerry device and the BlackBerry Enterprise Server. Only the BlackBerry Enterprise Server and the BlackBerry device can access the data that they send between them. Thus, third-parties, including service providers, cannot access potentially sensitive organization information in a decrypted format.

If the BlackBerry device cannot recognize the message format that the BlackBerry Enterprise Server decryption process produces, it does not receive the message; if the BlackBerry Enterprise Server receives a message encrypted with the wrong master encryption key, it does not send the message to the BlackBerry device. If message failure occurs, the BlackBerry device prompts the BlackBerry device user to generate a new master encryption key.

BlackBerry Enterprise Solution security features

Feature	Description
protect data	• Encrypt data traffic in transit between the BlackBerry Enterprise Server and the BlackBerry device. • Encrypt data traffic in transit between your organization's messaging and collaboration server and a BlackBerry device user's computer email application. • Use secure protocols to connect the BlackBerry Enterprise Server to the BlackBerry Infrastructure. • Encrypt data on the BlackBerry device. • Encrypt data in the BlackBerry Configuration Database. • Authenticate a BlackBerry device user to the BlackBerry device using a smart card with a password or passphrase. • Verify the authenticity and integrity of the BlackBerry device operating system and BlackBerry Device Software automatically.
protect encryption keys	• Encrypt encryption keys on the BlackBerry device.
control BlackBerry device connections	• Control which BlackBerry devices can connect to the BlackBerry Enterprise Server. • Control Bluetooth® connections to and from the BlackBerry device. • Control BlackBerry Smart Card Reader connections. • Control Wi-Fi® enabled BlackBerry device connections to enterprise Wi-Fi networks.

Feature	Description
control BlackBerry device and BlackBerry Desktop Software functionality	• Send wireless commands to turn on and turn off BlackBerry device functionality, delete information from BlackBerry devices, and lock BlackBerry devices. • Send IT policies to BlackBerry devices to customize security settings for BlackBerry device users or groups of BlackBerry device users on a BlackBerry Enterprise Server. • Send application control policies to BlackBerry devices to control third-party application availability and connections. • Enforce BlackBerry device and BlackBerry Smart Card Reader passwords.

New security features

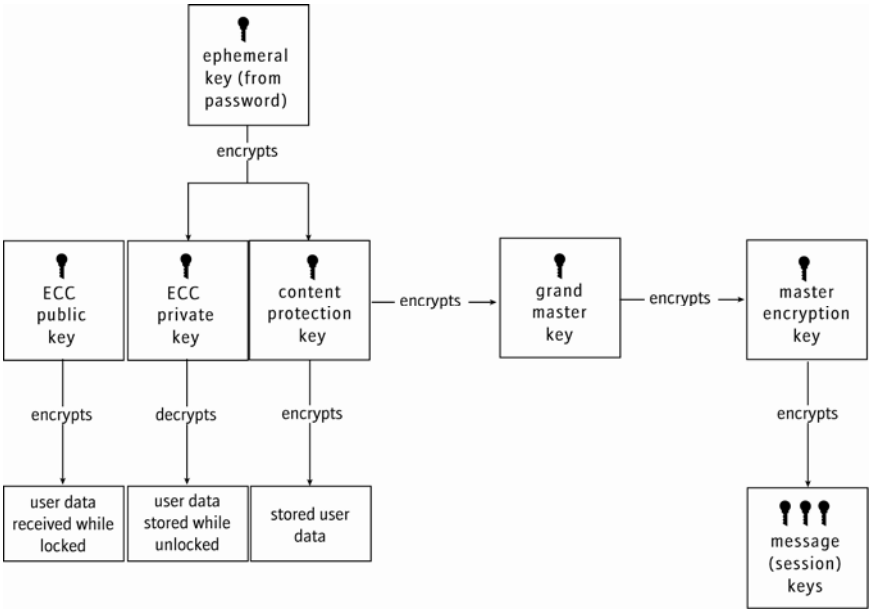
Feature	Software versions supported	Description
Wi-Fi enabled BlackBerry devices that include an RSA® SecurID cryptographic library support two-factor authentication with Wi-Fi enterprise networks.	• BlackBerry Enterprise Server Version 4.1 SP4 or later • BlackBerry Device Software Version 4.2.2 or later	Supported BlackBerry devices use the RSA SecurID® library and RSA implemented cryptography to create a passcode for use with a two-factor authentication process on the BlackBerry device.
Wireless software upgrade communication between supported BlackBerry devices and the BlackBerry Enterprise Solution components that send requests for wireless software upgrades to BlackBerry devices is designed to be protected.	• BlackBerry Enterprise Server Version 4.1 SP4 or later • BlackBerry Device Software Version 4.5 or later	Specific types of communication that the BlackBerry device receives from the BlackBerry Enterprise Server or BlackBerry Infrastructure contain a digital signature that the BlackBerry device uses to authenticate the messages.
BlackBerry devices running the S/MIME Support Package for BlackBerry devices or the PGP® Support Package for BlackBerry devices allow users to view encrypted attachments in S/MIME-protected and PGP protected messages.	• BlackBerry Enterprise Server Version 4.1 SP5 or later • BlackBerry Device Software Version 4.5 or later	The BlackBerry Enterprise Server administrator can use the S/MIME Allowed Encrypted Attachment Mode IT policy rule and the PGP Allowed Encrypted Attachment Mode IT policy rule to specify the least restrictive mode that the BlackBerry device can use to retrieve PGP encrypted and S/MIME-encrypted attachment information.
The BlackBerry Enterprise Server supports enhanced control of lost and stolen BlackBerry devices.	• BlackBerry Enterprise Server Version 4.1 SP5 or later • BlackBerry Device Software Version 4.5 or later	The BlackBerry Enterprise Server administrator can specify a delay (in hours) when using the Erase Data And Disable Handheld IT administration command over the wireless network.

Feature	Software versions supported	Description
The BlackBerry Enterprise Solution allows administrators to apply an encoding scheme to BlackBerry data using transcoder application code.	• BlackBerry Enterprise Server Version 4.1 SP5 or later • BlackBerry Device Software Version 4.5 or later	Third-party application developers can create encoding schemes that encrypt, convert, or otherwise change the format of BlackBerry device data.

BlackBerry encryption keys

By default, the BlackBerry Enterprise Solution generates the master encryption key and message key that the BlackBerry Enterprise Server and BlackBerry devices use to encrypt and decrypt all data traffic between them.

The BlackBerry Enterprise Server administrator can also enable the BlackBerry device to generate and use the content protection key to encrypt BlackBerry device user data while the BlackBerry device is locked, and generate and use the grand master key to encrypt the master encryption key while the BlackBerry device is locked.



Encryption key relationships on the BlackBerry device

Master encryption keys

The master encryption key is unique to the BlackBerry device. To send and receive messages, the master encryption key stored on the BlackBerry Enterprise Server and on the BlackBerry device must match. If the stored keys do not match, the BlackBerry device and the BlackBerry Enterprise Server cannot decrypt and must therefore discard messages that they receive.

Where master encryption keys are stored

The BlackBerry Configuration Database, the messaging server, and the BlackBerry device flash memory store encryption keys, including the current BlackBerry device master encryption key.

Messaging server platform	Messaging server storage location	BlackBerry device storage location	BlackBerry Enterprise Server storage location
IBM® Lotus® Domino®	the BlackBerry profiles database	a key store database in flash memory	the BlackBerry Configuration Database
Microsoft® Exchange	the computer email application user mailbox	a key store database in flash memory	the BlackBerry Configuration Database
Novell® GroupWise®	not stored	a key store database in flash memory	the BlackBerry Configuration Database

The BlackBerry Configuration Database stores master encryption keys alongside the BlackBerry device user data that they protect. The BlackBerry Configuration Database, the messaging server, and the BlackBerry device flash memory can also retain previous and pending master encryption keys. It is critical to protect the BlackBerry Configuration Database and the platform-specific master encryption key storage location on the messaging server. For more information, see "Messaging server to computer email application connection" on page 42 and "Protecting the BlackBerry Configuration Database" on page 34.

Key storage on the BlackBerry device

On the BlackBerry device, the shared key is stored in a database in flash memory (the key store). This key storage method is designed to prevent an attacker from extracting the key data from flash memory successfully by backing up the data from the BlackBerry device onto a computer.

Key state	Description
previous key(s)	The master encryption key(s) that the BlackBerry device used before the current key was generated. The BlackBerry device stores multiple previous keys in flash memory for 7 days, the maximum amount of time that the BlackBerry Enterprise Server queues a pending message for delivery, in case the BlackBerry device user creates a new key on the BlackBerry device multiple times while messages are still queued on the BlackBerry Enterprise Server. The messaging server and the BlackBerry Configuration Database store only the most recent previous key.
pending key	The master encryption key that the BlackBerry Enterprise Server administrator generates in the BlackBerry Manager to replace the current master encryption key. Only the messaging server and the BlackBerry Configuration Database store the pending key. The BlackBerry Desktop Software sends the pending key to the BlackBerry device when the BlackBerry device user connects the BlackBerry device to the computer. The current key then becomes the new previous key, and the pending key becomes the new current key.

How the messaging server storage location stores the master encryption keys

The Microsoft Exchange server stores the master encryption keys in a hidden folder named BlackBerryHandheldInfo within a root folder of the BlackBerry device user's computer email application mailbox. The BlackBerryHandheldInfo folder stores the following data:

- a message of class RIM.BlackBerry.Handheld.Config containing the BlackBerry device user's configuration information, including the master encryption key data
- the master encryption keys in binary form with tags that indicate their state: 0x6002 (pending), 0x6003 (current), and 0x6004 (previous)

The IBM Lotus Domino server stores the master encryption keys in a database named BlackBerryProfiles.nsf that contains configuration information for every BlackBerry device user within the /Data directory. The BlackBerry

Profiles database stores an account record containing the field RIMCurrentEncryptionKeyText, which stores the master encryption keys in alphanumeric representation of a hexadecimal string, for every BlackBerry device user.

How master encryption keys are generated

Both the BlackBerry Enterprise Server administrator and a BlackBerry device user can generate and regenerate master encryption keys. By default, the BlackBerry Enterprise Server sends a request to the BlackBerry Desktop Software every 31 days to prompt users to regenerate the master encryption key on their BlackBerry devices. If the user sets the Generate keys manually option in the BlackBerry Desktop Manager, the BlackBerry Enterprise Server still sends a key regeneration request to the BlackBerry Desktop Software automatically.

Key generation method	Initial key generation	Key regeneration
desktop based (wired)	When a BlackBerry device user connects the BlackBerry device to the computer for the first time, the BlackBerry Desktop Software creates the master encryption key and sends it to the BlackBerry device and the messaging server.	When the BlackBerry device user subsequently connects the BlackBerry device to the computer, the user can initiate regeneration of the master encryption key. The BlackBerry Desktop Software creates the master encryption key and sends it to the BlackBerry device and the messaging server.
wireless	Wireless enterprise activation permits a BlackBerry device user to remotely activate a BlackBerry device on the BlackBerry Enterprise Server without a physical network connection. During the wireless enterprise activation, the BlackBerry Enterprise Server and the BlackBerry device negotiate to select the strongest algorithm that they both support and use that algorithm to generate the master encryption key. **Note**: For more information, see "Authentication during wireless enterprise activation" on page 40.	On the BlackBerry device, a user can request a new master encryption key. The BlackBerry device sends the key regeneration request to the BlackBerry Enterprise Server over the wireless network. In the BlackBerry Manager, the BlackBerry Enterprise Server administrator can initiate regeneration of a master encryption key for a BlackBerry device.

Computer based process for generating master encryption keys

In BlackBerry Desktop Software Version 4.0 or later, the master encryption key generation function uses the current time as the seed for the C language srand function. The master encryption key generation function then gathers entropy (randomness) using the following process:

1. When prompted by the BlackBerry Desktop Software, the BlackBerry device user moves the mouse. The BlackBerry Desktop Software master encryption key generation function examines the lowest 12 bits of the x and y coordinates of the new mouse location. If the bits are different from the previous sample, the BlackBerry Desktop Software stores them, generating 3 bytes of randomness. If the bits are the same as the previous sample, no sample is taken.
2. The BlackBerry Desktop Software master encryption key generation function waits for a random interval between 50 and 150 milliseconds, and then continues to sample in the same way until it gathers 384 bytes.
3. The BlackBerry Desktop Software retrieves 384 bytes of randomness from the MSCAPI, for a total of 768 bytes.
4. The BlackBerry Desktop Software hashes the 384 bytes of randomness from the BlackBerry device user's mouse coordinates and the 384 bytes of randomness from the MSCAPI with SHA-512 to produce 512 bits of data. The BlackBerry Desktop Software frees the memory associated with the unused bits.

5. The BlackBerry Desktop Software uses the first 256 bits if it is generating the master encryption key using AES encryption or the first 128 bits if it is generating the master encryption key using Triple DES encryption. The BlackBerry Desktop Software discards any unused bits.

BlackBerry Enterprise Server versions earlier than 4.0 use a different desktop based master encryption key generation process. For more information, see "Appendix C: Previous version of wired master encryption key generation" on page 73.

Process for generating master encryption keys over the wireless network

To establish and manage master encryption keys over the wireless network, the BlackBerry Enterprise Server uses the initial key establishment protocol and the key rollover protocol. Both protocols provide strong authentication: only a BlackBerry device with a valid work email address and an activation password can initiate wireless enterprise activation and master encryption key generation.

Protocol	Description
initial key establishment protocol	• The BlackBerry Enterprise Server uses this protocol during wireless enterprise activation to establish the initial master encryption key. • This protocol uses SPEKE to initialize a key generation process using an activation password, enabling a BlackBerry device to establish long term public keys and a strong, cryptographically protected connection with a BlackBerry Enterprise Server.
key rollover protocol	• The BlackBerry device and the BlackBerry Enterprise Server use this protocol to regenerate a master encryption key, based on the existing master encryption key. When a BlackBerry device user physically connects the BlackBerry device to the computer, if a pending key exists, the current master encryption key on the BlackBerry device becomes a previous key and the pending key replaces the current key. If no pending key exists, the BlackBerry Desktop Software creates a new master encryption key for the user. • This protocol generates the master encryption key using existing long-term public keys and the ECMQV algorithm to negotiate a common key in such a way that an unauthorized party cannot calculate the same key. • This protocol achieves perfect forward secrecy. The new master encryption key is independent of the previous key. Knowledge of the previous master encryption key does not permit an attacker to learn the new master encryption key.

For more information about the wireless master encryption key generation protocols, see "Authentication during wireless enterprise activation" on page 40.

Message keys

The BlackBerry Enterprise Server and the BlackBerry device generate one or more message keys, which are designed to protect the integrity of data such as short keys or large messages, for each message that they send. If a message contains several datagrams and exceeds 2 KB, the BlackBerry Enterprise Server and the BlackBerry device generate a unique message key for each datagram.

Each message key is comprised of random information, which makes it difficult for a third party to decrypt, re-create, or duplicate the key.

The message key is a session key; the BlackBerry device does not store the message key persistently but frees the memory associated with it after using it in the decryption process.

Process for generating message keys on the BlackBerry Enterprise Server

The BlackBerry Enterprise Server is designed to seed a DSA PRNG function to generate a message key using the following process:

1. The BlackBerry Enterprise Server obtains random data from multiple sources for the seed, using a technique derived from the initialization function of the ARC4 encryption algorithm.
2. The BlackBerry Enterprise Server uses the random data to permute the contents of a 256-byte (2048-bit) state array.

   If the MSCAPI exists on the computer on which the BlackBerry Enterprise Server is running, the BlackBerry Enterprise Server also requests 512 bits of randomness from the MSCAPI to increase the amount of entropy.
3. The BlackBerry Enterprise Server inputs the state array into the ARC4 algorithm to further randomize the array.
4. The BlackBerry Enterprise Server draws 521 bytes from the ARC4 state array.

   Note: The BlackBerry Enterprise Server draws the additional 9 bytes (512 + 9=521) to make sure that the pointers before and after the call are not in the same place, and to take into account that the first few bytes of the ARC4 state array might not be truly random.
5. The BlackBerry Enterprise Server uses SHA-512 to hash the 521-byte value to 64 bytes.
6. The BlackBerry Enterprise Server uses the 64-byte value to seed a NIST-approved DSA PRNG function. For more information about the DSA PRNG function, see *Federal Information Processing Standard – FIPS PUB 186-2*.

   The BlackBerry Enterprise Server stores a copy of the seed in a file. When the BlackBerry Enterprise Server restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. The DSA PRNG function generates 128 pseudo-random bits for use with Triple DES and 256 pseudo-random bits for use with AES.
8. The BlackBerry Enterprise Server uses the pseudo-random bits with the appropriate algorithm to generate the message key.

Process for generating message keys on the BlackBerry device

The BlackBerry device is designed to seed a DSA PRNG function to generate a message key using the following process:

1. The BlackBerry device obtains random data from multiple sources for the seed, using a technique derived from the initialization function of the ARC4 encryption algorithm.
2. The BlackBerry device uses the random data to permute the contents of a 256-byte (2048-bit) state array.
3. The BlackBerry device inputs the state array into the ARC4 algorithm to further randomize the array.
4. The BlackBerry device draws 521 bytes from the ARC4 state array.

   Note: The BlackBerry device draws the additional 9 bytes (512 + 9=521) to make sure that the pointers before and after the call are not in the same place, and to take into account that the first few bytes of the ARC4 state array might not be truly random.
5. The BlackBerry device uses SHA-512 to hash the 521-byte value to 64 bytes.
6. The BlackBerry device uses the 64-byte value to seed a NIST-approved DSA PRNG function. For more information about the DSA PRNG function, see *Federal Information Processing Standard – FIPS PUB 186-2*.

   The BlackBerry device stores a copy of the seed in a file. When the BlackBerry device restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.

7. The DSA PRNG function generates 128 pseudo-random bits for use with Triple DES and 256 pseudo-random bits for use with AES.
8. The BlackBerry device uses the pseudo-random bits with the appropriate algorithm to generate the message key.

Content protection keys

When the BlackBerry Enterprise Server administrator turns on or the BlackBerry device user turns on content protection on the BlackBerry device, the BlackBerry device generates encryption keys, including the content protection key, that are designed to encrypt the user data on the BlackBerry device when the BlackBerry device is locked.

During the encryption process that begins when the BlackBerry device is locked, the BlackBerry device frees the memory that it associates with the content protection key and the ECC private key that it stores in RAM. The BlackBerry device then uses the ECC public key, an asymmetric key, to encrypt new BlackBerry device user data that it receives.

When the BlackBerry device is unlocked, the BlackBerry device decrypts the content protection key and the ECC private key in flash memory. The BlackBerry device then uses the ECC private key and the content protection key to decrypt user data on the BlackBerry device.

For more information, see "Protected storage of user data on a locked BlackBerry device" on page 28.

Process for generating content protection keys

When the BlackBerry Enterprise Server administrator turns on or the BlackBerry device user turns on content protection of data for the first time, the following process occurs:

1. The BlackBerry device uses the NIST-approved DSA PRNG to randomly generate the content protection key, a semi-permanent 256 bit AES encryption key.
2. The BlackBerry device generates an ECC key pair of a bit length that the BlackBerry device user or the BlackBerry Enterprise Server administrator determines.
3. The BlackBerry device prompts the user to type the BlackBerry device password.
4. The BlackBerry device derives an ephemeral 256 bit AES encryption key from the BlackBerry device password, in accordance with PKCS #5 (the password based cryptography standard). For more information, see "Appendix E: Ephemeral AES encryption key derivation process" on page 76.
5. The BlackBerry device uses the ephemeral key to encrypt the content protection key and the ECC private key.
6. The BlackBerry device stores the encrypted content protection key, the encrypted ECC private key, and the ECC public key in flash memory.

   If the BlackBerry device user changes the BlackBerry device password, the BlackBerry device uses the new password to derive a new ephemeral key and uses the new ephemeral key to re-encrypt the encrypted versions of the content protection key and the ECC private key in flash memory.

Process for encrypting user data on an unlocked BlackBerry device

The unlocked BlackBerry device uses the content protection key to encrypt data that the user types or otherwise adds on the BlackBerry device, or that the BlackBerry device receives.

Process for encrypting user data on a locked BlackBerry device

1. The BlackBerry device locks. When the BlackBerry device locks for the first time after the BlackBerry Enterprise Server administrator turns on or the BlackBerry device user turns on content protection, it uses the content protection key to automatically encrypt the bulk of its stored user and application data.
2. The BlackBerry device frees the memory associated with the decrypted content protection key and the decrypted ECC private key stored in RAM.

3. The locked BlackBerry device uses the ECC public key to encrypt data that it receives.

Process for decrypting user data on an unlocked BlackBerry device

1. A user types the correct BlackBerry device password to unlock the BlackBerry device.
2. The BlackBerry device uses the BlackBerry device password to derive the ephemeral 256 bit AES encryption key again.
3. The BlackBerry device uses the ephemeral key to decrypt the encrypted content protection key and the encrypted ECC private key in flash memory.
4. The BlackBerry device stores the decrypted content protection key and the decrypted ECC private key in RAM.
5. If the BlackBerry device user attempts to access user data that the BlackBerry device encrypted while it was unlocked, the BlackBerry device uses the decrypted content protection key to decrypt the user data.
6. If a BlackBerry device user attempts to access user data (for example, opens a message) that the BlackBerry device encrypted while it was locked, the BlackBerry device uses the decrypted ECC private key to decrypt the user data and access the ECC-encrypted items (for example, message bodies, subjects, or recipients).
7. When the BlackBerry device has opened 128 ECC-encrypted items (typically, less than 40 messages), the BlackBerry device uses the ECC private key to decrypt the ECC-encrypted items and then re-encrypts them with the content protection key the next time that the BlackBerry device locks. If the re-encryption process is incomplete when the BlackBerry device user next unlocks the BlackBerry device, the BlackBerry device resumes re-encryption when it locks again.

Grand master keys

When the BlackBerry Enterprise Server administrator turns on content protection of master encryption keys, the BlackBerry device uses a grand master key to encrypt the master encryption keys stored on the BlackBerry device in flash memory. When the BlackBerry device receives data encrypted with a master encryption key while it is locked, it uses the grand master key to decrypt the required master encryption key in flash memory and receive the data.

For more information, see "Protected storage of master encryption keys on a locked BlackBerry device" on page 31.

Process for generating grand master keys

When the BlackBerry Enterprise Server administrator turns on content protection of master encryption keys on the BlackBerry device for the first time, the following process occurs:

1. The BlackBerry device generates the grand master key, a 256 bit AES encryption key.
2. The BlackBerry device stores the decrypted grand master key in RAM.
3. The BlackBerry device uses the existing content protection key to encrypt the grand master key.
4. The BlackBerry device stores the encrypted grand master key in flash memory.
5. The BlackBerry device uses the decrypted grand master key to encrypt the master encryption keys stored in BlackBerry device flash memory.

BlackBerry symmetric key encryption algorithms

A symmetric key encryption algorithm is designed so that only the parties who know the secret key can decrypt the encrypted data or cipher text of the scrambled message.

The BlackBerry Enterprise Solution uses a symmetric key encryption algorithm to protect all data that the BlackBerry device sends or receives, while the data is in transit between the BlackBerry device and the BlackBerry Enterprise Server. This standard BlackBerry encryption, which is designed to provide strong security,

verifies that a BlackBerry message remains protected in transit to the BlackBerry Enterprise Server while the message data is outside your organization's firewall.

The BlackBerry Enterprise Solution uses either the Triple DES or the AES algorithm for standard BlackBerry encryption. By default, the BlackBerry Enterprise Server is set to use the strongest common symmetric key encryption algorithm, of either Triple DES or AES, that both the BlackBerry Enterprise Server and the BlackBerry device support.

Encryption algorithm	Description
Triple DES	The BlackBerry Enterprise Solution uses three iterations of the DES algorithm with two 56-bit keys in outer CBC mode for an overall key length of 112 bits. For more information, see *Federal Information Processing Standard - FIPS PUB 81 [3]*. In the two-key Triple DES algorithm, the first key encrypts the data, the second key decrypts the data, and then the first key encrypts the data again. Message keys and master encryption keys that the BlackBerry Enterprise Solution produces using Triple DES contain 112 bits of key data and 16 bits of parity data, which are stored as a 128-bit long binary string. Each parity bit is stored in the least significant bit of each of the 8 bytes of key data.
AES	A competition to design an algorithm with a better combination of security and performance than DES or Triple DES produced AES. AES offers a larger key size than DES or Triple DES to provide greater security against brute-force attacks. The BlackBerry Enterprise Solution uses AES with 256-bit keys in CBC mode to encrypt data that the BlackBerry Enterprise Server and the BlackBerry device send between them. The BlackBerry device implementation of AES includes power analysis and electromagnetic analysis countermeasure protection that is designed to address the potential of side-channel attacks against the BlackBerry device. The AES implementation uses masking countermeasures to hide the true operations taking place on the BlackBerry device so that power analysis readings or electromagnetic radiation emissions do not reveal information that can expose the encryption key. For more information, see "Appendix F: Power and electromagnetic side-channel attacks and countermeasures" on page 77. The AES message keys and master encryption keys that the BlackBerry Enterprise Solution uses contain 256 bits of key data.

When the BlackBerry device supports AES, the BlackBerry Enterprise Solution uses AES for BlackBerry transport layer encryption by default. Visit www.blackberry.com/knowledgecenterpublic/ to view the article KB-05429 "What Is - Recommendation on the use of Triple DES or AES for BlackBerry transport layer encryption" for more information on how the BlackBerry Enterprise Server uses AES transport layer encryption for all communication with BlackBerry devices.

Software requirements for BlackBerry encryption algorithms

Encryption algorithm	BlackBerry Enterprise Server	BlackBerry Device Software	BlackBerry Desktop Software
Triple DES	any version	any version	any version
AES	4.0 or later	4.0 or later	4.0 or later

If the BlackBerry Enterprise Server is set to permit the use of both Triple DES and AES and a BlackBerry device user is running the BlackBerry Device Software or the BlackBerry Desktop Software Version 3.7 or earlier, the BlackBerry Enterprise Solution generates that user's BlackBerry device master encryption keys using Triple DES. Otherwise, the BlackBerry Enterprise Solution generates master encryption keys using AES.

Standard BlackBerry message encryption

Standard BlackBerry encryption is designed to encrypt messages that the BlackBerry device sends or that the BlackBerry Enterprise Server forwards to the BlackBerry device. Standard BlackBerry encryption encrypts the message

- from the time a user sends an email message from the BlackBerry device until the BlackBerry Enterprise Server receives the message
- from the time the BlackBerry Enterprise Server receives a message sent to a BlackBerry device user until that user reads the message on the BlackBerry device

When a user sends a message from the BlackBerry device, the BlackBerry Enterprise Server does not encrypt the message when it forwards the message to the message recipient unless the BlackBerry device user installs additional secure messaging technology on the BlackBerry device and the BlackBerry Enterprise Server administrator has enabled the BlackBerry device to use that secure messaging technology to extend the messaging security. For more information, see "Extending BlackBerry device messaging security" on page 22.

Process for standard BlackBerry message encryption

When a user sends a message from the BlackBerry device, the BlackBerry device and BlackBerry Enterprise Server use symmetric key cryptography to encrypt and decrypt the message, using the following process:

1. The BlackBerry device compresses the message.
2. The BlackBerry device encrypts the message using the message key.
3. The BlackBerry device encrypts the message key using the master encryption key, which is unique to that BlackBerry device.
4. The BlackBerry device sends the encrypted message key and the encrypted message.
5. The BlackBerry Enterprise Server receives the encrypted message key and the encrypted message from the BlackBerry device.
6. The BlackBerry Enterprise Server decrypts the message key using the BlackBerry device master encryption key.
7. The BlackBerry Enterprise Server decrypts the message using the message key.
8. The BlackBerry Enterprise Server decompresses the message, and then forwards the message to the intended recipient.

When a BlackBerry device user receives a message, the following occurs:

1. The BlackBerry Enterprise Server receives the message.
2. The BlackBerry Enterprise Server compresses the message.
3. The BlackBerry Enterprise Server encrypts the message using the message key.
4. The BlackBerry Enterprise Server encrypts the message key using the user's BlackBerry device master encryption key.
5. The BlackBerry Enterprise Server sends the encrypted message and the encrypted message key to the user's BlackBerry device.
6. The BlackBerry device receives the encrypted message and the encrypted message key.
7. The BlackBerry device decrypts the message key using the master encryption key, which is unique to that BlackBerry device.
8. The BlackBerry device decrypts the message using the message key.
9. The BlackBerry device decompresses the message, rendering it readable by the BlackBerry device user.

Permitting third-party applications to encode BlackBerry device data

The BlackBerry Enterprise Server and the BlackBerry Device Software support a Transcoder API. This API permits third-party application developers to create encoding schemes that encrypt, convert, or otherwise change the format of data, and apply an encoding scheme to BlackBerry device data using transcoder application code. The third-party encoding scheme prepends a transcoder ID to the data that it encodes. The BlackBerry Enterprise Solution then encrypts the transcoder-encoded data using standard BlackBerry encryption.

The BlackBerry Enterprise Solution permits only third-party encoding schemes that the RIM signing authority system has digitally signed using the RIM Cryptographic API public key to access the Transcoder API to create the transcoder application code. To apply the third-party encoding scheme, the BlackBerry device must be running corresponding transcoder application code.

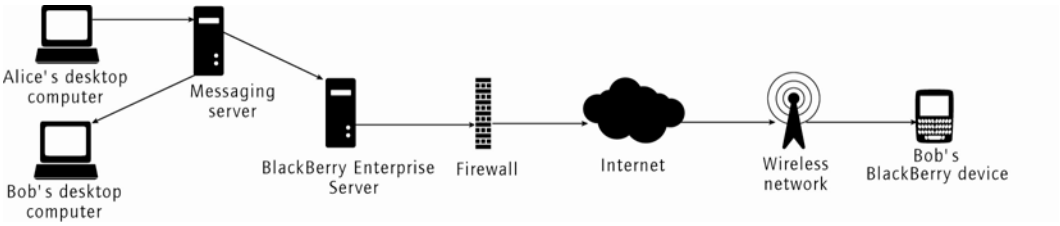
Third-party application developers can use the Transcoder API to add cryptographic components that the RIM Cryptographic API does not support by default to their third-party encoding schemes. The BlackBerry Enterprise Solution applies the third-party encoding schemes to any outgoing data to which standard BlackBerry encryption applies. The Transcoder API supports use of all the cryptography that the RIM Cryptographic API supports.

If the BlackBerry Enterprise Server administrator allows third-party applications to use the Transcoder API on the BlackBerry device, those applications, if not functioning correctly, might impact the security, usability and performance of the BlackBerry Enterprise Solution, and might cause loss of BlackBerry device data. To use the third-party encoding scheme, the BlackBerry Enterprise Server administrator must use the Security Transcoder Cod File Hashes IT policy rule to specify the .cod file for the third-party encoding scheme that the BlackBerry device permits to register as a transcoder. For more information about using the Security Transcoder Cod File Hashes IT policy rule, see the *Policy Reference Guide*.

BlackBerry wireless messaging security

The BlackBerry Enterprise Solution is designed with advanced security features to work seamlessly with existing networks while enabling BlackBerry device users to securely send and receive messages while away from their computers. Email messages remain encrypted at all points between the BlackBerry devices and the BlackBerry Enterprise Server.

Receiving an email message on the BlackBerry device



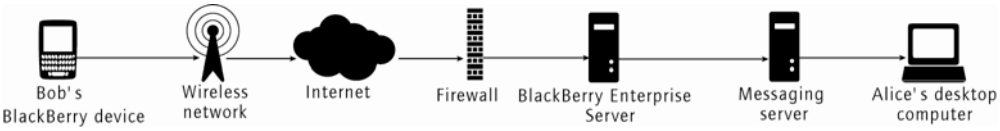
Sending a message from a computer to the BlackBerry device

1. Alice sends a message to Bob from her computer. Alice and Bob work at the same organization.
2. The messaging server receives the email message and notifies the BlackBerry Enterprise Server that the message has arrived.
3. The messaging server delivers the message to Bob's computer.
4. The BlackBerry Enterprise Server retrieves the message from the messaging server.
5. The BlackBerry Enterprise Server queries the messaging server for BlackBerry device user preferences to determine whether or not to forward the message to Bob's BlackBerry device.
6. The BlackBerry Enterprise Server compresses and encrypts the message.
7. The BlackBerry Enterprise Server places the message in the outgoing queue.

The BlackBerry Enterprise Server is designed to maintain a constant, direct outbound TCP/IP connection to the wireless network over the Internet through the firewall on port 3101 (or 4101 in the case of a BlackBerry device that supports implementation alongside an enterprise Wi-Fi network). This constant connection enables the efficient, continuous delivery of data to and from the BlackBerry device.

8. The wireless network routes and then delivers the encrypted message to Bob's BlackBerry device.
9. Bob's BlackBerry device receives the encrypted message. The BlackBerry device then decrypts and displays the message for Bob to read.

Sending an email message from the BlackBerry device



Sending a message from a BlackBerry device to the computer

1. Bob responds to Alice's message by composing an email on the BlackBerry device. When Bob sends the message, the BlackBerry device compresses, encrypts, and then sends the message over the wireless network.

   All messages that users create on their BlackBerry devices contain the necessary BlackBerry Enterprise Server routing information for the wireless network to make sure that the wireless network delivers the message to the appropriate BlackBerry Enterprise Server.
2. The BlackBerry Infrastructure routes the encrypted message to the BlackBerry Enterprise Server on which the BlackBerry device user resides.

   The connection from the BlackBerry Enterprise Server to the BlackBerry Infrastructure is a two-way TCP connection on port 3101. The BlackBerry Infrastructure directs messages from the BlackBerry device to this connection using the routing information in the message.
3. The BlackBerry Enterprise Server receives the message.
4. The BlackBerry Enterprise Server decrypts, decompresses, and sends the message to the messaging server.

   The BlackBerry Enterprise Server does not store a copy of the message.
5. The messaging server delivers the message to Alice's computer.

Message attachment viewing security features

The BlackBerry device supports attachment viewing through the BlackBerry Attachment Service. The BlackBerry Attachment Service enables users to perform the following actions on their BlackBerry devices:

- view Microsoft® PowerPoint® slide shows, including those in .pps file format
- view .bmp, .jpg, .jpeg, .gif, .png, .tif, .tiff, and .wmf file formats
- view .doc, .dot, .txt .html, .htm, .pdf, .xls, .wpd, and .ppt documents in a browser
- open .zip files and then open any content files of supported formats
- open .wav files
- enlarge images in .tiff format (such as scanned documents or faxes)
- access inline thumbnail images for attachments that are embedded in messages

The BlackBerry Attachment Service is designed to prevent malicious applications from accessing data on the BlackBerry device by using binary format parsing to open the attachments and prepare them to be sent to the BlackBerry device for rendering. The BlackBerry device does not run applications that are sent as attachments in email messages.

The system administrator can install the BlackBerry Attachment Service on a remote computer and then place that computer on its own network segment to prevent the spread of potential attacks from the BlackBerry Attachment Service to another computer within your organization's network. In a segmented network, attacks are isolated and contained on a single area of the network. Using segmented network architecture is designed to improve the security and performance of the BlackBerry Attachment Service network segment by filtering out attachment data that is not destined for other network segments. For more information about placing the BlackBerry Enterprise Solution components in a network architecture that is segmented, see *Placing the BlackBerry Enterprise Solution in a Segmented Network*.

Viewing attachments in PGP encrypted or S/MIME-encrypted messages

The BlackBerry Enterprise Server administrator can use the S/MIME Allowed Encrypted Attachment Mode IT policy rule and the PGP Allowed Encrypted Attachment Mode IT policy rule to specify the least restrictive mode that the BlackBerry device can use to retrieve PGP (OpenPGP (RFC 2440) or PGP/MIME (RFC 3156) message formatting) encrypted and S/MIME-encrypted attachment information.

When a user receives an OpenPGP encrypted message that includes an attachment, the BlackBerry Enterprise Server reads the attachment header data and is designed to send the message and the encrypted message key to the BlackBerry device automatically.

When a user receives a PGP/MIME encrypted or S/MIME-encrypted message that includes an attachment on the BlackBerry device, depending on the setting of the S/MIME Allowed Encrypted Attachment Mode IT policy rule or the PGP Allowed Encrypted Attachment Mode IT policy rule, the following actions can occur automatically when the user opens the message, or when the user requests the actions manually.

1. The BlackBerry device sends the message key and a request for the attachment header data to the BlackBerry Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the message and access the attachment header data.
3. The BlackBerry Enterprise Server sends the attachment header data to the BlackBerry device.
4. The BlackBerry device processes the attachment header data with the message and displays the associated attachment information so that the user can select the attachment for viewing.

When the user tries to view an attachment that is encrypted using S/MIME, PGP/MIME, or OpenPGP on the BlackBerry device, the following actions occur:

1. The BlackBerry device sends the message key and a request for the attachment data to the BlackBerry Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the message and access the attachment data that corresponds to the attachment header data.
3. The BlackBerry Enterprise Server decrypts the attachment and sends the rendered attachment data to the BlackBerry device.
4. The BlackBerry device displays the attachment.

Note: To protect the decrypted attachment data that the BlackBerry device stores, turn on content protection.

PIN-to-PIN messaging

A PIN uniquely identifies each BlackBerry device and BlackBerry enabled device on the wireless network. If a BlackBerry device user knows the PIN of another BlackBerry device, the user can send a PIN message to that BlackBerry device. Unlike an email message that the BlackBerry device user sends to an email address, a PIN message bypasses the BlackBerry Enterprise Server and your organization's network.

PIN message scrambling

During the manufacturing process, Research In Motion (RIM) loads a common peer-to-peer, or PIN-to-PIN, encryption key onto BlackBerry devices. Although the BlackBerry device uses the peer-to-peer encryption key

with Triple DES to encrypt PIN messages, every BlackBerry device can decrypt every PIN message that it receives because every BlackBerry device stores the same global peer-to-peer encryption key. This means that if a BlackBerry device or BlackBerry enabled device user other than the intended PIN message recipient intercepts a PIN message, that BlackBerry device or BlackBerry enabled device user can decrypt and read the PIN message using the global peer-to-peer encryption key. Therefore, consider PIN messages as scrambled, not encrypted, messages.

The BlackBerry Enterprise Server administrator can limit the number of BlackBerry devices that can receive and decrypt your organization's PIN messages by generating a new peer-to-peer encryption key known only to BlackBerry devices in your organization. A BlackBerry device with an organization-specific peer-to-peer encryption key can send and receive PIN messages with other BlackBerry devices on your organization's network with the same peer-to-peer encryption key only. These PIN messages use organization-specific scrambling instead of the default global scrambling.

The BlackBerry Enterprise Server administrator can also set the Firewall Block Incoming Messages IT policy rule to limit the number of BlackBerry devices in your organization that can receive either or both of PIN messages that use organization-specific scrambling and PIN messages that use the default global scrambling.

The BlackBerry Enterprise Server administrator should generate a new organization-specific peer-to-peer encryption key if the administrator knows the current key is compromised. The BlackBerry Enterprise Server administrator can update and resend the peer-to-peer encryption key for BlackBerry device users in the BlackBerry Manager.

Text messaging

Text messaging using SMS and MMS are available on some BlackBerry devices. Supported BlackBerry devices can send SMS and MMS messages over the wireless TCP/IP connection between them. The BlackBerry device does not encrypt text messages.

Controlling unsecured messaging

The BlackBerry Enterprise Server administrator can control unsecured messaging (PIN, SMS, and MMS communication) in your organization using the following IT policy rules:

IT policy rule	Description
Allow External Connections	This IT policy rule controls whether applications can initiate external connections (for example, to WAP, SMS, MMS or other public gateways) on the BlackBerry device.
Confirm on Send	This IT policy rule requires a BlackBerry device user to confirm that they wish to send the message before sending an email message, PIN message, SMS message, or MMS message.
Disable Forwarding Between Services	This IT policy rule prevents a BlackBerry device user from forwarding or replying to a message using a different BlackBerry Enterprise Server from the one that delivered the original message. This IT policy rule also prevents using an email account to forward or reply to a PIN message or reply to an email message with a PIN message.
Disable Peer-to-Peer Normal Send	This IT policy rule prevents a BlackBerry device user from sending plain text PIN messages when using a secure messaging package, such as the S/MIME Support Package for BlackBerry devices or the PGP Support Package for BlackBerry devices.
Firewall Block Incoming Messages	This IT policy rule limits the number of BlackBerry devices in your organization that can receive SMS messages, MMS messages, BlackBerry Internet Service messages, PIN messages that use organization-specific scrambling, and PIN messages that use the default global scrambling.

Turning off unsecured messaging

The BlackBerry Enterprise Server administrator can turn off unsecured messaging to make sure that all communication originating at BlackBerry devices in your organization travels through the enterprise messaging environment.

Scenario	Description
turn off PIN messaging	Set the Allow Peer-to-Peer Messages IT policy rule to **False**. **Note**: When the BlackBerry Enterprise Server administrator turns off PIN messaging, BlackBerry device users cannot send PIN messages from their BlackBerry devices; however, they can still receive PIN messages on their BlackBerry devices.
turn off SMS messaging	Set the Allow SMS IT policy rule to **False**.
turn off MMS messaging	Set the Disable MMS IT policy rule to **True**.

Extending BlackBerry device messaging security

In addition to standard BlackBerry encryption, the BlackBerry Enterprise Server administrator can enable S/MIME technology or PGP technology to offer an additional layer of security between the sender and recipient of an email or PIN message. Using either one of these technologies enables sender-to-recipient authentication and confidentiality, and helps maintain data integrity and privacy from the time that a BlackBerry device user sends a message from the BlackBerry device until the message recipient decodes and reads the message.

PGP Support Package for BlackBerry devices

The PGP Support Package for BlackBerry devices is designed to provide support for using OpenPGP (RFC 2440) and PGP/MIME (RFC 3156) message formatting on the BlackBerry device to enable BlackBerry device users who already send and receive PGP protected messages in OpenPGP and PGP/MIME formats using their computer email applications to send and receive PGP protected messages in these formats using their BlackBerry devices.

The PGP Support Package for BlackBerry devices includes tools for obtaining PGP keys and transferring them to the BlackBerry device so that BlackBerry devices with the PGP Support Package for BlackBerry devices installed can decrypt PGP protected messages and BlackBerry device users can read the decrypted messages on their BlackBerry devices. Users can digitally sign, encrypt, and send PGP protected messages from their BlackBerry devices. Without the PGP Support Package for BlackBerry devices, the BlackBerry device receives PGP protected messages as unreadable cipher text.

Within the PGP Universal environment, the PGP Universal Server operates as a network appliance. The PGP Universal Server specifies secure email policies that the PGP Universal Server administrator designs. The BlackBerry device with the PGP Support Package for BlackBerry devices installed enforces compliance with the PGP Universal secure email policies for all email messages.

The PGP Support Package for BlackBerry devices is designed to include support for the following features:

- using the PGP Universal Server to retrieve and enforce a secure email policy
- searching for and retrieving PGP keys, PGP key status, and X.509 certificate status over the wireless network using either a PGP Universal Server or an external LDAP key server
- setting the BlackBerry device to connect to external LDAP PGP key servers using SSL/TLS (LDAPS) connections
- encrypting and decrypting PGP protected email and PIN messages
- verifying digital signatures on received email and PIN messages, and digitally signing outgoing email and PIN messages

The BlackBerry device is designed to use the BlackBerry MDS Connection Service, which resides on the BlackBerry Enterprise Server, to connect to the PGP Universal Server and to the external LDAP PGP key server(s) that the BlackBerry device user sets on the BlackBerry device. The Connection Service uses standard protocols, such as HTTP and TCP/IP, to enable the BlackBerry device to retrieve PGP keys and PGP key status from the PGP Universal Server or an external LDAP PGP key server over the wireless network.

PGP security

PGP technology is designed to enable sender-to-recipient authentication and confidentiality and help maintain data integrity and privacy from the time that the BlackBerry device user sends a message over the wireless network until the message recipient decodes and reads the message.

PGP technology relies on public key cryptography (using private and public key pairs) to provide confidentiality, integrity and authenticity.

PGP key types

The PGP Support Package for BlackBerry devices uses public key cryptography with the following keys:

Key type	Description
PGP public key	The BlackBerry device uses the recipient's PGP public key to encrypt outgoing email messages, and uses the sender's PGP public key to verify digital signatures on received email messages. The PGP public key is designed to be distributed and accessed by message recipients and senders without compromising security conditions.
PGP private key	The BlackBerry device uses the PGP private key to digitally sign outgoing email messages and decrypt received email messages. Private key information should remain private to the key owner.

PGP encryption

If the PGP Support Package for BlackBerry devices exists on a BlackBerry device, when a user sends a message from that BlackBerry device, the BlackBerry device encrypts the message using the following process:

1. The BlackBerry device encrypts the message using the message recipient's PGP public key.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the PGP encrypted message.
3. The BlackBerry device sends the encrypted message to the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server removes the standard BlackBerry encryption and sends the PGP encrypted message to the recipient.

If the PGP Support Package for BlackBerry devices exists on a BlackBerry device, when the BlackBerry device receives a message, the BlackBerry device decrypts the message using the following process:

1. The BlackBerry Enterprise Server receives the PGP protected message.
2. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the PGP encrypted message.
3. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
4. The BlackBerry device removes the standard BlackBerry encryption and stores the PGP encrypted message.
5. When the user opens the message on the BlackBerry device, the BlackBerry device decrypts the PGP encrypted message and renders the message contents.

PGP encryption algorithms

The BlackBerry device is designed to support the use of a strong algorithm for PGP encryption. The PGP Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported

algorithms to encrypt PGP messages. The BlackBerry Enterprise Server administrator can set the PGP Allowed Content Ciphers IT policy rule to encrypt PGP messages using any of AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), and Triple DES (168-bit).

The message recipient's PGP key indicates which content ciphers the recipient can support, and the BlackBerry device is designed to use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if the recipient's PGP key does not include a list of ciphers.

For more information, see the *PGP Support Package for BlackBerry Devices Security Technical Overview*.

S/MIME Support Package for BlackBerry devices

The S/MIME Support Package for BlackBerry devices is designed to enable BlackBerry device users who are already sending and receiving S/MIME messages using their computer email application to send and receive S/MIME-protected messages using their BlackBerry devices. The S/MIME Support Package for BlackBerry devices is designed to work with S/MIME email clients including Microsoft Outlook® and Microsoft Outlook Express, and with popular PKI components, including Netscape®, Entrust® Authority™ Security Manager version 5 and later, and Microsoft certificate authorities.

The S/MIME Support Package for BlackBerry devices includes tools for obtaining certificates and transferring them to the BlackBerry device. This means that BlackBerry devices with the S/MIME Support Package for BlackBerry devices installed can decrypt messages that are encrypted using S/MIME encryption and BlackBerry device users can read the decrypted messages on their BlackBerry devices, and that BlackBerry device users can sign, encrypt, and send S/MIME messages from their BlackBerry devices. Without the S/MIME Support Package for BlackBerry devices the BlackBerry Enterprise Server sends a message to the BlackBerry device in which the message body includes a statement that the S/MIME message cannot be decrypted.

The S/MIME Support Package for BlackBerry devices includes support for the following features:

- certificate and private key synchronization and management using the Certificate Synchronization Manager included in the BlackBerry Desktop Software
- encrypting and decrypting messages, including PIN messages, verifying digital signatures, and digitally signing outgoing messages
- searching for and retrieving certificates and certificate status over the wireless network using PKI protocols
- smart cards on BlackBerry devices

PKI component support

The S/MIME Support Package for BlackBerry devices is designed to support the following PKI components:

- LDAP: The BlackBerry device and the Certificate Synchronization Manager use LDAP or LDAPS to search for and download certificates.
- OCSP: The BlackBerry device and the Certificate Synchronization Manager use OCSP to check the revocation status of a certificate on demand.
- CRL: The BlackBerry device and the Certificate Synchronization Manager obtain the most recent revocation status of certificates, which is published at a frequency set on the certificate authority server, from a CRL.

S/MIME encryption

If the S/MIME Support Package for BlackBerry devices exists on a BlackBerry device, when the BlackBerry device user sends a message, the BlackBerry device encrypts the message using the following process:

1. The BlackBerry device encrypts the message with the S/MIME certificate of the message recipient.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the S/MIME-encrypted message.
3. The BlackBerry device sends the encrypted data to the BlackBerry Enterprise Server.

4. The BlackBerry Enterprise Server removes the standard BlackBerry encryption and sends the S/MIME-encrypted message to the recipient.

If the S/MIME Support Package for BlackBerry devices exists on a BlackBerry device, when the user receives a message on the BlackBerry device, the BlackBerry device decrypts the message using the following process:

1. The BlackBerry Enterprise Server receives the S/MIME-protected message.
2. If the message is signed-only or weakly encrypted, the BlackBerry Enterprise Server encrypts the message a second time with S/MIME encryption if the BlackBerry Enterprise Server administrator has turned on this option using the BlackBerry Manager.
3. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the S/MIME data.
4. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
5. The BlackBerry device removes the standard BlackBerry encryption and stores the S/MIME-encrypted message.
6. When the BlackBerry device user opens the message on the BlackBerry device, the BlackBerry device decrypts the S/MIME-encrypted message and renders the message contents.

S/MIME encryption algorithms

The BlackBerry device is designed to support the use of a strong algorithm for S/MIME encryption. When the BlackBerry Enterprise Server administrator turns on S/MIME encryption on the BlackBerry Enterprise Server, the S/MIME Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported algorithms (other than the two weakest RC2 algorithms, RC2 (64-bit) and RC2 (40-bit)) to encrypt S/MIME messages.

The BlackBerry Enterprise Server administrator can use the Weak Digest Algorithms IT policy rule to specify algorithms that BlackBerry devices consider weak. The BlackBerry device uses the list of weak digest algorithms when verifying that the digital signatures on messages that the BlackBerry device receives are not generated using a weak hash digest. The BlackBerry device uses the list of weak digest algorithms when verifying that the certificate chains for the certificates used to sign messages that the BlackBerry device receives do not contain hashes generated using a weak digest.

The BlackBerry Enterprise Server administrator can set the S/MIME Allowed Content Ciphers IT policy rule to allow the BlackBerry device to encrypt S/MIME messages using any of AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), RC2 (128-bit), Triple DES, RC2 (64-bit), and RC2 (40-bit).

If the BlackBerry device has previously received a message from the intended recipient, the BlackBerry device is designed to recall which content ciphers the recipient can support, and use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if it does not know the decryption capabilities of the recipient.

S/MIME certificates

When a BlackBerry device user sends an encrypted message from the BlackBerry device, the BlackBerry device uses the S/MIME certificate of the message recipient to encrypt the message.

When a BlackBerry device user receives a signed message, the BlackBerry device uses the S/MIME certificate of the message sender to verify the message signature.

S/MIME private keys

When a BlackBerry device user sends a signed message from the BlackBerry device, the BlackBerry device hashes the message using SHA-1, SHA-256, SHA-384, SHA-512, or MD5, and then uses the S/MIME private key of the BlackBerry device user to digitally sign the message hash.

When a BlackBerry device user receives an encrypted message, the BlackBerry device uses the private key of the user to decrypt the message.

For more information, see the *S/MIME Support Package for BlackBerry Devices Security Technical Overview*.

Decrypting and reading messages on the BlackBerry device using Lotus Notes API 7.0

The BlackBerry® Enterprise Server Version 4.1 or later for IBM® Lotus® Domino® with Lotus Notes® API 7.0 automatically turns on support for reading IBM Lotus Notes encrypted messages and S/MIME-encrypted messages on the BlackBerry device. Lotus Notes API 7.0 requires the BlackBerry device user's Notes .id file and password to decrypt the received secure messages. The BlackBerry device user must manually click Import Notes ID and attach a copy of the Notes .id file that they used to login. The IBM Lotus Domino messaging agent copies the Notes .id file to the BlackBerry Enterprise Server in plain text format temporarily, at the request of the Lotus Notes API.

If a BlackBerry device user has support for this feature turned on, when the BlackBerry device forwards or replies to an encrypted message that the BlackBerry device has received, decrypted, and decompressed, the BlackBerry Enterprise Server for IBM Lotus Domino decrypts the message before the BlackBerry device sends the message to the recipient as plain text.

The BlackBerry Enterprise Server administrator can configure the default BlackBerry device behaviour in the following ways:

- use the Disable Notes Native Encryption Forward And Reply IT policy rule to prevent BlackBerry device users from forwarding and replying to IBM Lotus Notes encrypted messages on their BlackBerry devices
- use the Notes Native Encryption Password Timeout IT policy rule to specify the maximum length of time (in minutes) that the BlackBerry device stores the IBM Lotus Notes .id password that the user types

Process for decrypting IBM Lotus Notes and S/MIME messages

If a BlackBerry device user sets support for reading IBM Lotus Notes and S/MIME-encrypted messages on the BlackBerry device, when the BlackBerry device user receives an IBM Lotus Notes or S/MIME-encrypted message, the BlackBerry Enterprise Server for IBM Lotus Domino decrypts the message using the following process:

1. A BlackBerry device user receives an IBM Lotus Notes and S/MIME-encrypted message.
2. The BlackBerry Enterprise Server for IBM Lotus Domino messaging agent decrypts the BlackBerry device user's cached Notes .id password and uses the decrypted password to decrypt the message.

   If the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent does not have the Notes .id password, the BlackBerry device user must select More, More All, or Open Attachment to pull the decrypted message to the BlackBerry device.
3. The BlackBerry Enterprise Server deletes the decrypted Notes .id password from memory. The encrypted Notes .id password remains cached.
4. The BlackBerry Enterprise Server pushes the decrypted message to the BlackBerry device, where the user can read the message.

Notes .id password protection

After a BlackBerry device user imports the Notes .id file and password (stored in the Notes .id file), the password is

- encrypted in BlackBerry device memory using AES with the BlackBerry device user's master encryption key
- encrypted in the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent memory using AES with the BlackBerry device user's master encryption key
- decrypted before being used to call the required Lotus Notes API security functions

The BlackBerry Enterprise Server for IBM Lotus Domino messaging agent deletes the Notes .id files and plain text passwords it stores when

- a message decryption failure occurs on the BlackBerry Enterprise Server
- the BlackBerry Enterprise Server restarts
- the password times out (the default expiration timeout is 24 hours)

The encrypted Notes .id password remains stored in the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent memory cache. The BlackBerry Enterprise Server administrator can customize the length of time for which the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent caches the password. The BlackBerry Enterprise Server administrator can also set the timeout value to 0 to require the BlackBerry device user to type the Notes .id password to decrypt and read every Lotus Notes encrypted message the user receives on the BlackBerry device. Visit www.blackberry.com/knowledgecenterpublic/ to view the article KB-12420 "How to – Change the length of time for which the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent caches a Notes .id password" for more information on customizing the length of time for which the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent caches the password.

The BlackBerry device deletes the Notes .id files and plain text passwords from BlackBerry device memory when

- a message decryption failure occurs on the BlackBerry device
- the BlackBerry device resets
- the password times out (the default expiration timeout period is 24 hours)

If a BlackBerry device user types more than ten consecutive incorrect passwords on the BlackBerry device within one hour, the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent makes secure messaging unavailable to that BlackBerry device user for one hour.

The temporary disabling period increases by ten minute increments to a limit of 24 hours. It increments each time a BlackBerry device user exceeds the maximum number of failed password attempts, and defaults back to one hour when the user types the correct password.

When secure messaging is temporarily unavailable, a BlackBerry device user can manually re-enable secure messaging by importing the Notes .id file, or changing the Notes .id password using the BlackBerry Desktop Software or the Domino Web Access client.

Protecting stored data

Protecting stored messages on the messaging server

The IBM Lotus Domino server and the Microsoft Exchange server perform all message storage and specific user data storage in their environments. In the Novell GroupWise server environment, the Post-Office Agent where a user's messaging account resides stores messages and user data.

Messaging server	Message storage location
IBM Lotus Domino server	IBM Lotus Domino databases within the IBM Lotus Domino environment
Microsoft Exchange server	Hidden folders in Microsoft Exchange mailboxes that are associated with a user

Storing message and user data in IBM Lotus Domino databases

The BlackBerry Enterprise Server creates and uses the following IBM Lotus Domino databases to manage BlackBerry device messages:

Database	Message storage method
BlackBerry state	Stores an entry that establishes a connection between each original message in a user's IBM Lotus Notes Inbox and the same message on that user's BlackBerry device Each BlackBerry device user has a uniquely named BlackBerry state database.

Database	Message storage method
BlackBerry profiles	• stores important configuration information for each BlackBerry device user, including the BlackBerry device identification information and master encryption key • stores a link to a user's BlackBerry state database and stores other information that the BlackBerry Enterprise Server uses to manage the flow of messages to and from the BlackBerry device

IT policy signing and storage on the BlackBerry device

An IT policy is a collection of one or more IT policy rules. An IT administration command is a function that the BlackBerry Enterprise Server administrator can send over the wireless network to immediately control access to or change ownership information on the BlackBerry device.

After the BlackBerry Enterprise Server installation process creates the BlackBerry Configuration Database, the BlackBerry Enterprise Server generates a unique private and public key pair to authenticate the IT policy and the IT administration commands, and digitally signs the Default IT policy before automatically sending it and the IT policy public key to the BlackBerry device.

The BlackBerry device stores the digitally signed IT policy and the IT policy public key in the NV store in flash memory, binding the IT policy to that particular BlackBerry device. The NV store persists in flash memory and can only be overwritten by the BlackBerry device operating system. Third-party application code cannot write to the NV store.

The BlackBerry Enterprise Server stores the IT policy private key in the BlackBerry Configuration Database. The BlackBerry Enterprise Server uses the IT policy private key to sign all IT policy packets that it sends to the BlackBerry device. The BlackBerry device uses the IT policy public key in the NV store to authenticate the digital signature on the IT policy.

Application password encryption and storage on the BlackBerry device

A BlackBerry device user can use the Password Keeper tool to create and store all of the passwords that they might use to gain access to applications and web sites on the BlackBerry device. This means that a BlackBerry device user is required to remember only the Password Keeper master password to retrieve all of their stored passwords.

The first time that a BlackBerry device user opens the Password Keeper on the BlackBerry device, the user must create the Password Keeper master password. The Password Keeper encrypts the information (for example, application and web site passwords and data) that it stores using 256-bit AES, and uses the master password to decrypt the information when a BlackBerry device user types the master password to gain access to the Password Keeper tool. The BlackBerry device automatically deletes all of its data if a user types the Password Keeper master password incorrectly ten times.

In the Password Keeper, a BlackBerry device user can

- type a password and its identifying information (for example, which application the BlackBerry device user can access using the password) and save the information
- generate random passwords designed to improve password strength
- copy passwords to the clipboard to be pasted into an application or web site password prompt

Protected storage of external memory on the BlackBerry device

The BlackBerry device is designed to encrypt multimedia data that it stores on an external memory device according to the External File System Encryption Level IT policy rule or the corresponding BlackBerry device setting.

The BlackBerry device is designed to support the following features:

- external file encryption by encrypting specific files on the external memory device using AES

  The external file system encryption does not apply to files that the BlackBerry device user manually transfers to external memory (for example, from a USB mass storage device).

- access control to objects on the external memory device using code signing with 1024-bit RSA

The external memory device stores encrypted copies of the file keys that the BlackBerry device is designed to use to decrypt and encrypt files on the external memory device. The BlackBerry device is designed to use a device key stored in the NV store in BlackBerry device RAM, a user-provided password, or both to encrypt the external memory file keys.

The BlackBerry device is designed to permit code signing keys in the header information of the encrypted file on the external memory device. The BlackBerry device is designed to check the code signing keys when the BlackBerry device opens the input or output streams of the encrypted file.

The BlackBerry device, any computer platform, and other devices that use the external memory device can modify encrypted files (for example, truncate files) on the external memory device. The BlackBerry device is not designed to perform integrity checks on the encrypted file data.

Process for generating external memory file encryption keys

When the BlackBerry Enterprise Server administrator turns on or the BlackBerry device user turns on encryption of external memory for the first time, the following process occurs:

1. The BlackBerry device generates a 32 byte AES encryption key.
2. The BlackBerry device stores the encryption key in the NV store in RAM on the BlackBerry device.
3. The BlackBerry device XoRs the AES key with another 32 byte AES encryption key that is encrypted using a password to generate the external memory file encryption key (a session key).
4. The BlackBerry device encrypts the external memory file encryption key using the AES encryption key.
5. The BlackBerry device stores the encrypted external memory file encryption key on the external memory device.

Process for encrypting files stored in external memory on the Blackberry device

When the BlackBerry device user stores a file in external memory for the first time after the BlackBerry Enterprise Server administrator turns on or the BlackBerry device user turns on mass media storage, the BlackBerry device decrypts the external memory file encryption key and uses it to automatically encrypt the stored file.

Protected storage of user data on a locked BlackBerry device

If content protection is turned on, BlackBerry device content is always protected with the 256-bit AES encryption algorithm. Content protection of BlackBerry device user data is designed to perform the following actions:

- use 256-bit AES to encrypt stored data when the BlackBerry device is locked
- use an ECC public key to encrypt data that the BlackBerry device receives when it is locked

When the BlackBerry Enterprise Server administrator or a BlackBerry device user turns on content protection on the BlackBerry device, the BlackBerry device uses content protection to encrypt the following user data items:

Item	Description
AutoText	all text that automatically replaces the text a BlackBerry device user types
BlackBerry Browser	• content that web sites or third-party applications push to the BlackBerry device • web sites that the user saves on the BlackBerry device • browser cache

Item	Description
calendar	• subject • location • organizer • attendees • notes included in the appointment or meeting request
contacts (in the address book)	all information except the contact title and category **Note**: Set the Force Include Address Book In Content Protection IT policy rule to True to prevent the BlackBerry device user from turning off the Include Address Book option on the BlackBerry device. The BlackBerry device permits the Caller ID and Bluetooth Address Book transfer features to work when content protection is turned on and the BlackBerry device is locked.
Email	• subject • email addresses • message body • attachments
memo list	• title • information included in the body of the note
OMA DRM applications	a key identifying the BlackBerry device and a key identifying the SIM card (if available) that the BlackBerry device adds to DRM forward-locked applications
RSA SecurID Library	the contents of the .sdtid file seed stored in flash memory
tasks	• subject • information included in the body of the task

Enabling protected storage of BlackBerry device data

The BlackBerry Enterprise Server administrator enables protected storage of data on the BlackBerry device by setting the Content Protection Strength IT policy rule. Choose a strength level that corresponds to the desired ECC key strength.

If a BlackBerry device user turns on content protection on the BlackBerry device, in the BlackBerry device Security Options, the BlackBerry device user can set the content protection strength to the same levels that the BlackBerry Enterprise Server administrator can set using the IT policy rule.

When the content-protected BlackBerry device decrypts a message that it received while locked, the BlackBerry device uses the ECC private key in the decryption operation. The longer the ECC key, the more time the ECC decryption operation adds to the BlackBerry device decryption process. Choose a content protection strength level that optimizes either the ECC encryption strength or the decryption time.

If the BlackBerry Enterprise Server administrator sets the content protection strength to Stronger (to use a 283-bit ECC key) or to Strongest (to use a 571-bit ECC key), consider setting the Minimum Password Length IT policy rule to enforce a minimum BlackBerry device password length of 12 characters or 21 characters, respectively. These password lengths maximize the encryption strength that the longer ECC keys are designed to provide. The BlackBerry device uses the BlackBerry device password to generate the ephemeral 256-bit AES encryption key that the BlackBerry device uses to encrypt the content protection key and the ECC private key. A weak password produces a weak ephemeral key.

For more information, see "Process for generating content protection keys" on page 14.

Protected storage of master encryption keys on a locked BlackBerry device

If the BlackBerry Enterprise Server administrator turns on content protection of master encryption keys, the BlackBerry device uses the grand master key to encrypt the master encryption keys stored in flash memory and encrypts the grand master key using the content protection key. When the BlackBerry device receives data encrypted with a master encryption key while it is locked, it uses the decrypted grand master key to decrypt the required master encryption key in flash memory, and uses the decrypted master encryption key to decrypt and receive the data.

The BlackBerry device stores the decrypted master encryption keys and the decrypted grand master key in RAM only. When the BlackBerry Enterprise Server administrator, the BlackBerry device user, or a set password timeout locks the BlackBerry device, the wireless transceiver remains on and the BlackBerry device does not clear the RAM associated with these keys. The BlackBerry device is designed to prevent the decrypted grand master keys and the decrypted master encryption keys from appearing in flash memory.

For more information, see "Process for generating grand master keys" on page 15.

Enabling protected storage of master encryption keys on a locked BlackBerry device

The BlackBerry Enterprise Server administrator enables protected storage of master encryption keys on the BlackBerry device by setting the Force Content Protection of Master Keys IT policy rule. When the BlackBerry Enterprise Server administrator turns on content protection of master encryption keys, the BlackBerry device uses the same ECC key strength that it uses to encrypt BlackBerry device user and application data when encrypting the master encryption keys. For more information, see "Enabling protected storage of BlackBerry device data" on page 30.

Protected storage of master encryption keys on a BlackBerry device during a reset

If the BlackBerry Enterprise Server administrator turns on content protection of master encryption keys, during a BlackBerry device reset the BlackBerry device

- turns off the wireless transceiver
- turns off serial bypass
- frees the memory associated with all data and encryption keys stored in RAM, including the decrypted grand master key
- locks

The wireless transceiver and serial bypass are designed to be turned off while the content protection key is not available to decrypt the grand master key in flash memory. Until a user unlocks the BlackBerry device using the correct BlackBerry device password the BlackBerry device cannot receive and decrypt data.

When the user unlocks the BlackBerry device after a reset, the BlackBerry device

- uses the content protection key to decrypt the grand master key in flash memory
- stores the decrypted grand master key in RAM again
- re-establishes the wireless connection to the BlackBerry Infrastructure
- resumes serial bypass
- receives data from the BlackBerry Enterprise Server

Clearing the BlackBerry device memory

By default, the BlackBerry device continually runs a standard Java garbage collection process to reclaim BlackBerry device memory that is no longer referenced.

If secure garbage collection is turned on, the BlackBerry device performs the following additional actions:

- overwrites the memory reclaimed by the standard garbage collection process with zeroes

- periodically runs the memory cleaner application, which tells BlackBerry device applications to empty any caches and free memory associated with unused, sensitive application data
- automatically overwrites the memory freed by the memory cleaner application when it runs

Any of the following conditions enable the BlackBerry device to perform secure garbage collection:

- content protection is turned on
- an application uses the RIM Cryptographic Application Programming Interface (Crypto API) to create a private or symmetric key
- a third-party application turns on secure garbage collection by registering with the memory cleaner
- S/MIME Support Package for BlackBerry devices is installed
- PGP Support Package for BlackBerry devices is installed

Setting memory clearing options

BlackBerry device users can set the memory cleaner application to run when their BlackBerry devices are holstered or when their BlackBerry devices remain idle for a set period of time. BlackBerry device users can also manually run the memory cleaner application on their BlackBerry devices, run specific registered memory cleaners in the BlackBerry device Security Options, and turn the memory cleaner application on and off. If secure garbage collection is turned on, when the memory cleaner application runs, it invokes the secure garbage collection process.

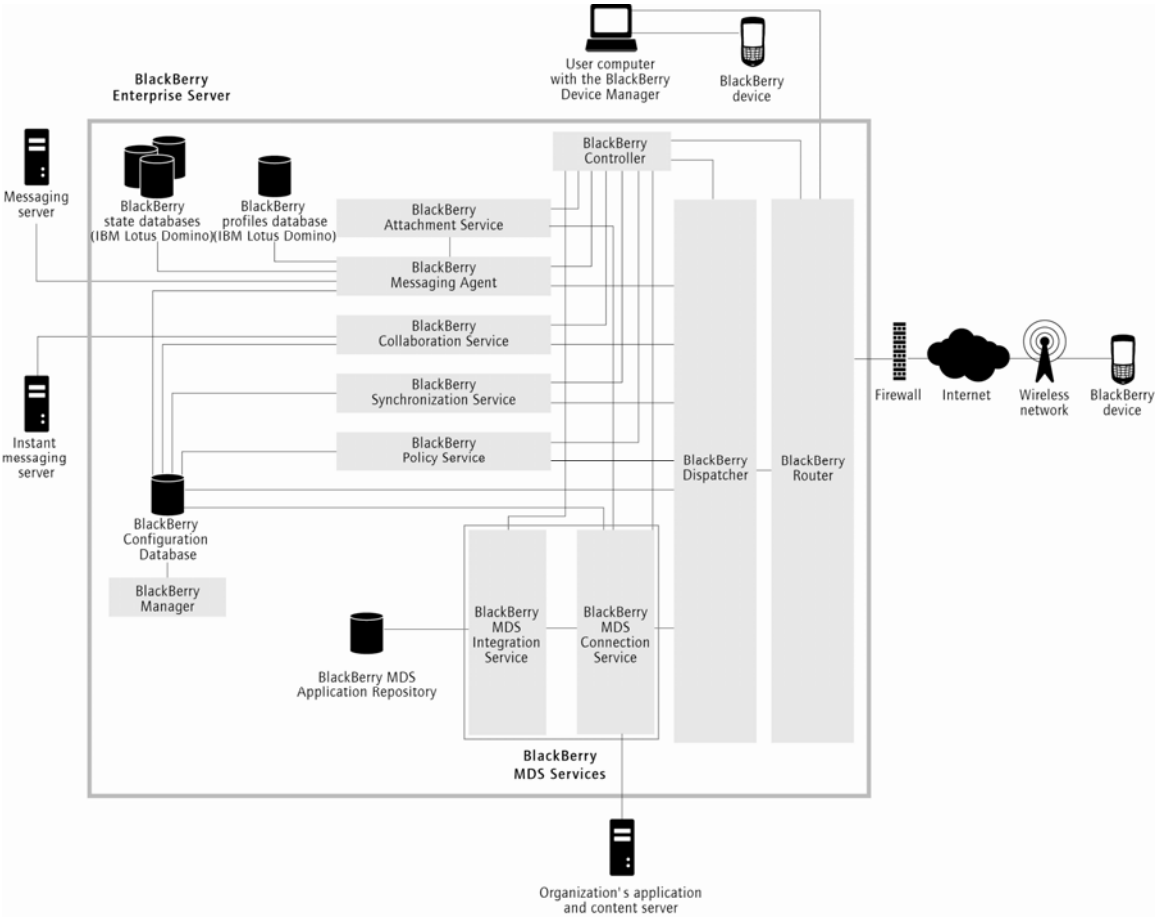
The BlackBerry Enterprise Server administrator can set the memory cleaner application to run automatically when the following actions occur:

- BlackBerry device user synchronizes the BlackBerry device with the computer
- BlackBerry device user locks the BlackBerry device
- BlackBerry device locks after a specified amount of idle time
- BlackBerry device user changes the time or time zone on the BlackBerry device

For more information, see the *Policy Reference Guide*.

BlackBerry architecture component security

The BlackBerry Enterprise Server consists of services that provide functionality and components that monitor services and processes, route, compress, and encrypt data, and communicate with the BlackBerry Infrastructure over the wireless network.



BlackBerry Enterprise Server architecture

For more information on the BlackBerry Enterprise Server architecture, see the *BlackBerry Enterprise Server Feature and Technical Overview*.

To improve the security and performance of the BlackBerry Enterprise Solution services and components, the system administrator can separate your organization's network into multiple firewall-segmented components to create a network architecture that is segmented. Each segment of your organization's network can contain network traffic destined for a specific component or service. For more information about placing the BlackBerry Enterprise Solution components in a network architecture that is segmented, see *Placing the BlackBerry Enterprise Solution in a Segmented Network*.

BlackBerry Infrastructure

The BlackBerry Infrastructure is designed to communicate with the BlackBerry Enterprise Server using a RIM-proprietary protocol called Server Routing Protocol (SRP). SRP is a point-to-point protocol that runs over TCP/IP.

BlackBerry Enterprise Server

The BlackBerry Enterprise Server is designed to establish a secure, two-way link between a BlackBerry device user's work email account and that user's BlackBerry device. The BlackBerry Enterprise Server uses this link to complete message delivery within the protection of your organization's firewall.

Messaging server

The BlackBerry Enterprise Solution is designed to interoperate with messaging servers such as Microsoft Exchange, IBM Lotus Domino, and Novell GroupWise. The BlackBerry Enterprise Solution is designed to use existing messaging server security without altering the normal functionality of the messaging server. The messaging server continues to receive, deliver, and store all email messages, while the BlackBerry Enterprise Server acts as a conduit to transfer these messages to and from the BlackBerry device.

BlackBerry Configuration Database

The BlackBerry services that do not connect to the messaging server directly access the configuration information that a SQL database (the BlackBerry Configuration Database) stores. BlackBerry services that might otherwise require access to the messaging server can access encryption keys and passwords through the BlackBerry Configuration Database to perform many tasks.

The BlackBerry Configuration Database stores the following information:

- BlackBerry Enterprise Server names
- unique SRP authentication keys and unique SRP IDs, or UIDs, that each BlackBerry Enterprise Server uses in the SRP authentication process to establish a connection to the wireless network
- IT policy private keys of the IT policy public and private key pair that the BlackBerry Enterprise Server generates for each BlackBerry device
- PIN of each BlackBerry device
- read-only copies of each unique BlackBerry device master encryption key
- BlackBerry device user lists
- information contained in the message header that the BlackBerry Enterprise Server sends, for example, message ID, date, and message status, (BlackBerry Enterprise Server for IBM Lotus Domino only)
- a semi-permanent reference to user data using the GroupWise MessageID in the MBMailSync, MBCalendarSync, MBPIMSync, and MBFolderSync database synchronization tables (BlackBerry® Enterprise Server for Novell® GroupWise® only)

Protecting the BlackBerry Configuration Database

Your environment might benefit from configuring the Microsoft® SQL Server™ for optimal security of the BlackBerry Configuration Database and protection of the stored BlackBerry device user encryption keys.

Configuration option	Recommendations
shield your Microsoft SQL Server installation from Internet based attacks	• Require Windows Authentication Mode for connections to Microsoft SQL Server to restrict connections to Microsoft® Windows® user and domain user accounts and enable credentials delegation. Windows Authentication Mode eliminates the need to store passwords on the client side. However, if your organization is running the BlackBerry MDS Services, your SQL server must support Mixed Mode authentication. • Use Windows security enforcement mechanisms such as stronger authentication protocols and mandatory password complexity and expiration.
Password-protect the service account	Assign a string password to your sa account, even on servers that require Windows Authentication. A string password is designed to prevent exposure of a blank or weak sa password if the server is ever reset for Mixed Mode Authentication.
Limit the privilege level of Microsoft SQL Server Windows services	Associate each service with a Windows account from which the service derives its security context. Microsoft SQL Server allows a user of the sa login and in some cases other users to access operating system features derived from the security context of the account that owns the server process. If the server is not secured, a malicious user might use these operating system calls to extend an attack to any other resource to which the Microsoft SQL Server service account has access.
Use the Microsoft SQL Server Enterprise Manager	• If your organization must change the account associated with a Microsoft SQL Server service, the system administrator should use the SQL Server Enterprise Manager to do so. The SQL Server Enterprise Manager sets the appropriate permissions on the files and registry keys that the Microsoft SQL Server uses. • Do not use the Microsoft Management Console Services applet to change the account associated with a Microsoft SQL Server service. Using this Services applet requires the system administrator to manually adjust many registry and NTFS file system permissions and Microsoft Windows user rights. For more information, see the Microsoft Knowledge Base article *How to change the SQL Server or SQL Server Agent service account without using SQL Enterprise Manager in SQL Server 2000 or SQL Server Management Studio in SQL Server 2005*.
Make the Microsoft SQL Server ports that are monitored by default on your firewall unavailable	Set your firewall to filter out packets that are addressed to TCP port 1433, addressed to UDP port 1434, or associated with named instances.

Configuration option	Recommendations
Use a secure file system	• Use NTFS for the Microsoft SQL Server because it is more stable and recoverable than FAT file systems, and enables security options such as file and directory ACLs and EFS. • Do not change the permissions that the Microsoft SQL Server sets during installation. The Microsoft SQL Server sets appropriate ACLs on registry keys and files if it detects NTFS. • If the system administrator must change the account that runs the Microsoft SQL Server, decrypt the files under the old account and re-encrypt them under the new account.
Delete unsecured, old setup files	Delete Microsoft SQL Server setup files that might contain plain text, credentials encrypted with weak public keys, or sensitive configuration information that the Microsoft SQL Server logged to a Microsoft SQL Server version-dependent location during installation. **Note**: Microsoft distributes a free tool, Killpwd, which is designed to locate and delete passwords from unsecured, old setup files on your system. For more information, see the Microsoft Knowledge Base article *Service Pack Installation May Save Standard Security Password in File*.
Audit connections to the Microsoft SQL Server	• At a minimum, log failed connection attempts to the Microsoft SQL Server and review the log regularly. • When possible, save log files to a different hard drive than the one on which data files are stored.

Changing the BlackBerry Configuration Database

If the BlackBerry Enterprise Server administrator moves the BlackBerry device to a BlackBerry Enterprise Server that uses a different BlackBerry Configuration Database, the BlackBerry Enterprise Server administrator or a BlackBerry device user must permanently delete all BlackBerry device user and application data, the BlackBerry device master encryption key, and the IT policy public key from the BlackBerry device. For more information, see "Remotely erasing data from BlackBerry device memory and making the BlackBerry device unavailable" on page 62.

The BlackBerry Enterprise Server administrator or the BlackBerry device user must initiate regeneration of a new, unique master encryption key. The new BlackBerry Enterprise Server must generate a unique IT policy private and public key pair and digitally sign and send the Default IT policy and the IT policy public key to the BlackBerry device before the BlackBerry device can communicate with the new BlackBerry Enterprise Server.

The new BlackBerry Configuration Database stores the new BlackBerry Enterprise Server name and the BlackBerry device master encryption key and IT policy private key.

BlackBerry MDS Services databases

The BlackBerry MDS Services store their database access credentials in plain text form in INSTALL_DIR\BlackBerry MDS Services 4.1.0\jakarta-tomcat-5.5.9\conf\server.xml. To protect the access credentials in that storage location, the system administrator must

- use a separate SQL login account to install and manage the BlackBerry MDS Services databases
- assign read and write control to that location to a separate BlackBerry MDS Services SQL login account only

For more information, see the *BlackBerry Enterprise Server Installation Guide*.

Protecting the BlackBerry Enterprise Solution connections

The BlackBerry Enterprise Server is designed to communicate with the BlackBerry Infrastructure using SRP authentication to establish a connection to the wireless network. The BlackBerry Enterprise Server contacts the BlackBerry Infrastructure to establish an initial connection using SRP.

The BlackBerry Enterprise Server and the BlackBerry Infrastructure perform an authentication handshake when they attempt to establish a connection. If the authentication fails, they do not establish a connection. If a BlackBerry Enterprise Server uses the same unique SRP authentication key and unique SRP ID to connect to (and then disconnect from) the BlackBerry Infrastructure five times in one minute, the BlackBerry Infrastructure disables that SRP ID to prevent a malicious user using the same SRP ID (for example, to try to create a Denial of Service condition).

After the BlackBerry Enterprise Server and the BlackBerry Infrastructure establish an initial connection over the Internet, the BlackBerry Enterprise Server uses a persistent TCP/IP connection to send data to the BlackBerry Infrastructure. The BlackBerry Infrastructure uses standard protocols to send data to the BlackBerry device.

A BlackBerry device can bypass SRP connectivity and authentication by using the BlackBerry Router to connect directly to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server can communicate with the BlackBerry Router using a combination of the SRP and BlackBerry Router authentication protocols.

SRP authentication

SRP is designed to perform the following actions when the BlackBerry Enterprise Server and BlackBerry Infrastructure establish an authenticated connection and subsequently transfer data between one another over the wireless network:

- authenticate the BlackBerry Infrastructure to the BlackBerry Enterprise Server and the BlackBerry Enterprise Server to the BlackBerry Infrastructure
- exchange configuration information between the BlackBerry Enterprise Server and the BlackBerry Infrastructure

The BlackBerry Infrastructure and the BlackBerry Enterprise Server authenticate with each other before they can transfer data. The authentication handshake sequence depends on a shared secret encryption key (the SRP authentication key) on both the BlackBerry Enterprise Server and the BlackBerry Infrastructure. If at any point in the authentication handshake sequence the authentication fails, SRP terminates the connection.

The BlackBerry Enterprise Server is designed to send a basic information packet to the BlackBerry Infrastructure immediately following the initial SRP authentication process. The packet format is designed to be recognizable to both the BlackBerry Enterprise Server and the BlackBerry Infrastructure, enabling both sides to set the parameters of the SRP implementation dynamically.

To support backward compatibility with older versions of the BlackBerry Enterprise Server, which terminate the SRP connection if they receive unrecognized packets, the BlackBerry Infrastructure does not send basic information packets to the BlackBerry Enterprise Server until the BlackBerry Enterprise Server has sent a packet of the same format to the BlackBerry Infrastructure.

SRP authentication process

Step	Action	Description
1	The BlackBerry Enterprise Server sends its SRP ID, or UID, to the BlackBerry Infrastructure.	The BlackBerry Enterprise Server sends a packet to the BlackBerry Infrastructure to claim its own UID.
2	The BlackBerry Infrastructure sends a challenge string to the BlackBerry Enterprise Server.	The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Enterprise Server.

Step	Action	Description
3	The BlackBerry Enterprise Server sends a challenge string to the BlackBerry Infrastructure.	When the BlackBerry Enterprise Server receives the BlackBerry Infrastructure challenge string, it sends a challenge string to the BlackBerry Infrastructure.
4	The BlackBerry Infrastructure sends a challenge response to the BlackBerry Enterprise Server.	The BlackBerry Infrastructure hashes the BlackBerry Enterprise Server challenge string with the SRP authentication key, a 20-byte shared secret encryption key, using the keyed HMAC with SHA-1. The BlackBerry Infrastructure sends the resulting 20-byte value back to the BlackBerry Enterprise Server.
5	The BlackBerry Enterprise Server sends a challenge response to the BlackBerry Infrastructure.	The BlackBerry Enterprise Server responds to the BlackBerry Infrastructure challenge string by hashing the challenge with the shared SRP authentication key.
6	The BlackBerry Infrastructure sends an acceptance to the BlackBerry Enterprise Server.	When the BlackBerry Infrastructure accepts the challenge response, it sends a final confirmation to the BlackBerry Enterprise Server to complete the authentication process and set up an authenticated SRP connection between the BlackBerry Infrastructure and the BlackBerry Enterprise Server. If the BlackBerry Infrastructure rejects the response, the connection fails and SRP closes the authentication session.

How the BlackBerry Enterprise Server and the BlackBerry Infrastructure handle undeliverable messages

When a party sends a message to a BlackBerry device, the BlackBerry Infrastructure might not be able to deliver the message to the BlackBerry device immediately in the following scenarios:

Scenario	Result
The BlackBerry device state prevents the BlackBerry device from sending and receiving messages over the wireless network. The BlackBerry device user might change the BlackBerry device state by moving in and out of wireless coverage or turning the BlackBerry device on and off, preventing message delivery.	• The message expires if the message remains undelivered after the timeout value set on the BlackBerry Infrastructure (7 days) elapses or the connection to the BlackBerry Enterprise Server is lost. The BlackBerry Infrastructure informs the source that the message could not be delivered. • If the BlackBerry Infrastructure receives a message to a BlackBerry device that it cannot deliver after trying for 10 minutes, the BlackBerry Infrastructure informs the BlackBerry Enterprise Server and deletes the message. • The BlackBerry Enterprise Server requests notification from the BlackBerry Infrastructure of when the BlackBerry device changes state. When the BlackBerry device state indicates that it can send and receive messages over the wireless network, the BlackBerry Infrastructure notifies the BlackBerry Enterprise Server and the BlackBerry Enterprise Server sends any pending messages to the BlackBerry device.

Scenario	Result
The connection between the BlackBerry Enterprise Server and the BlackBerry Infrastructure terminates.	• The BlackBerry Infrastructure informs the source BlackBerry device that the message could not be delivered and deletes the message after trying for 10 minutes. • When the connection is re-established, the BlackBerry Enterprise Server resends the undelivered message to the recipient BlackBerry device. If more than five messages are pending, the BlackBerry Enterprise Server stores them in the BlackBerry Configuration Database.

BlackBerry Router protocol authentication

The BlackBerry Router is designed to bypass the SRP authenticated connection to the BlackBerry Infrastructure to route data to BlackBerry devices that are connected to the BlackBerry Device Manager through a physical connection to a computer or BlackBerry devices that are connected over port 4101 to an enterprise Wi-Fi network. Data that BlackBerry devices and the BlackBerry Router send between one another is compressed and encrypted.

The system administrator can install the BlackBerry Router on a remote computer to route data traffic between the BlackBerry Infrastructure and one or more BlackBerry Enterprise Servers. The BlackBerry device must authenticate itself to the BlackBerry Enterprise Server to prove that it knows the master encryption key before the BlackBerry Router sends data to the BlackBerry device. The BlackBerry Enterprise Server and the BlackBerry device use the BlackBerry Router protocol to open a mutually authenticated connection between them.

When the authentication process used by the BlackBerry Router protocol is successful, the BlackBerry device sends data to the BlackBerry Router through the BlackBerry Device Manager or over port 4101 to an enterprise Wi-Fi network, and the BlackBerry Router sends data to the BlackBerry device through the BlackBerry Device Manager or over port 4101 to an enterprise Wi-Fi network. When the BlackBerry device user disconnects the BlackBerry device from the computer or closes the BlackBerry Device Manager, or disconnects from the enterprise Wi-Fi network, the wireless data flow over the SRP connection is restored. The BlackBerry Enterprise Server and the BlackBerry Router use the BlackBerry Router protocol to close the authenticated connection to the BlackBerry device.

Authentication process used by the BlackBerry Router protocol

Step	Action	Description
1	A BlackBerry device user physically connects a BlackBerry device to a computer, or connects a BlackBerry device to an enterprise Wi-Fi network.	The user connects the BlackBerry device to a computer that is running the BlackBerry Device Manager, or connects the BlackBerry device to an enterprise Wi-Fi network.
2	The BlackBerry Router authenticates the BlackBerry device.	The BlackBerry Enterprise Server and the BlackBerry device use the unique BlackBerry Router authentication protocol to verify that the BlackBerry device has the correct master encryption key. The value of the master encryption key that the BlackBerry device and the BlackBerry Enterprise Server share is not available to the BlackBerry Router. The BlackBerry Enterprise Server and the BlackBerry device use the same authentication information to validate each other that the SRP authentication handshake sequence uses to determine whether or not the BlackBerry Enterprise Server can connect to the BlackBerry Infrastructure.

For more information about the BlackBerry Router protocol and the authentication process, see "Masking operation process that the AES implementation uses when content protection is turned on" on page 77.

Authentication during wireless enterprise activation

Wireless enterprise activation enables a BlackBerry device user to activate a supported BlackBerry device on the BlackBerry Enterprise Server without a physical connection to a computer. The BlackBerry Enterprise Server administrator can use wireless enterprise activation to implement a large number of BlackBerry devices remotely.

Wireless enterprise activation produces a master encryption key that authenticates a BlackBerry device user and secures the communication between the BlackBerry Enterprise Server and the BlackBerry device. The BlackBerry Enterprise Server and the BlackBerry device use an initial key establishment protocol that uses SPEKE to initialize a key generation process using an activation password to establish a shared master encryption key that enables strong authentication between them.

After the BlackBerry device successfully activates on the BlackBerry Enterprise Server, the BlackBerry device no longer requires the activation password. The BlackBerry device user (or another user) cannot reuse that password to activate another BlackBerry device.

Authentication process used during wireless enterprise activation

Step	Action	Description
1	A BlackBerry device user initiates the wireless enterprise activation process.	The user opens the enterprise activation application on the BlackBerry device and types their work email address and the activation password that the BlackBerry Enterprise Server administrator communicated to them.
2	The BlackBerry device sends an activation request to the BlackBerry Infrastructure.	The BlackBerry device sends an activation request to the BlackBerry Infrastructure using standard BlackBerry protocols. The BlackBerry Infrastructure uses SMTP to send an activation message to the BlackBerry device user's email account. This activation message contains BlackBerry device routing information and public keys.
3	The BlackBerry Enterprise Server sends an activation response to the BlackBerry device.	The BlackBerry Enterprise Server sends the BlackBerry device an activation response that contains BlackBerry Enterprise Server routing information and public keys.
4	The BlackBerry Enterprise Server and the BlackBerry device establish and verify the shared master encryption key.	The BlackBerry Enterprise Server and the BlackBerry device use the initial key establishment protocol to establish a master encryption key. The BlackBerry Enterprise Server and the BlackBerry device verify the master encryption key with each other. If the BlackBerry Enterprise Server and the BlackBerry device mutually confirm the correct master encryption key, the activation proceeds, and the BlackBerry Enterprise Server and the BlackBerry device use the master encryption key to encrypt further communication between one another.
5	The BlackBerry Enterprise Server sends service books to the BlackBerry device.	The BlackBerry Enterprise Server sends the appropriate service books to the BlackBerry device. The BlackBerry device user can now send messages from and receive messages on the BlackBerry device.

Step	Action	Description
6	The BlackBerry Enterprise Server sends data to the BlackBerry device.	If wireless PIM synchronization and wireless backup is enabled for the BlackBerry device user, the BlackBerry Enterprise Server sends the following data to the user's BlackBerry device: • calendar entries • contacts, tasks, and memos • existing BlackBerry device options (if applicable) that the BlackBerry device backed up using automatic wireless backup.

For more information, see the *BlackBerry Wireless Enterprise Activation Technical Overview*.

TCP/IP connection

The TCP/IP connection from the BlackBerry Enterprise Server to the BlackBerry Router is designed to be secure in the following ways:

Security measure	Description
The BlackBerry Enterprise Server sends outbound traffic to the BlackBerry device only through the authenticated connection to the BlackBerry Infrastructure.	The system administrator must set your organization's firewall or proxy to permit the BlackBerry Enterprise Server to initiate and maintain an outbound connection to the BlackBerry Infrastructure on TCP port 3101.
The BlackBerry Enterprise Server does not send inbound-initiated traffic to the messaging server.	The BlackBerry Enterprise Server discards inbound traffic from any source other than the BlackBerry device (through the BlackBerry Infrastructure or BlackBerry Desktop Software) or the messaging server.
The BlackBerry Enterprise Solution encrypts data traffic over TCP/IP.	• Data remains encrypted with standard BlackBerry encryption from the BlackBerry Enterprise Server to the BlackBerry device or from the BlackBerry device to the BlackBerry Enterprise Server. There is no intermediate point at which the data is decrypted and encrypted again. • No data traffic of any kind can occur between the BlackBerry Enterprise Server and the wireless network or the BlackBerry device unless the BlackBerry Enterprise Server can decrypt the data using the correct, valid master encryption key. Only the BlackBerry device and BlackBerry Enterprise Server have the correct, valid master encryption key.
The BlackBerry Enterprise Server encrypts data traffic between specific components	The BlackBerry Collaboration Service, the Connection Service, the BlackBerry Policy Service, and the BlackBerry Synchronization Service share a secure communication password that is known only to them. The BlackBerry Messaging Agent and the BlackBerry Dispatcher share a different secure communication password that is known only to them. When one of these components initiates a connection to the BlackBerry Dispatcher, the BlackBerry inter-process protocol is designed to use SPEKE to initialize a key generation process using the component's secure communication password and establishes a 256-bit AES encryption key (a session key). The BlackBerry Enterprise Server then uses the session key to encrypt data traffic to any components that store the same secure communication password.

Security measure	Description
The BlackBerry device initiates inbound connections using the BlackBerry Router to an enterprise Wi-Fi network only.	The BlackBerry Router sends the Internet or intranet content requests from the BlackBerry device over port 4101 to the enterprise Wi-Fi network. The BlackBerry Router verifies that the PIN belongs to a valid BlackBerry device that is registered on the wireless network.

Messaging server to computer email application connection

The system administrator can set your messaging server to encrypt the BlackBerry device data in transit between the messaging server and the BlackBerry device user's computer email application.

Messaging server	Data traffic encryption method
IBM Lotus Domino	• The BlackBerry Enterprise Server and the IBM Lotus Domino server communicate using the same IBM Lotus Notes RPC to enable seamless communication between the BlackBerry Enterprise Server, BlackBerry-related IBM Lotus Domino databases, and the IBM Lotus Domino server. • Users that activate their BlackBerry devices using physical connections to their computers can encrypt data traffic in transit between the IBM Lotus Domino server and their IBM Lotus Notes Inboxes. For more information, see the IBM Lotus Domino help files.
Microsoft Exchange	• The BlackBerry Enterprise Server and the Microsoft Exchange Server communicate using the same Microsoft Exchange server RPC. • BlackBerry device users can use 128-bit encryption to encrypt RPC communication over the MAPI connection between the Microsoft Exchange Server and Microsoft Outlook. For more information on enabling encryption in Microsoft Windows, see the Microsoft product documentation.
Novell GroupWise	The BlackBerry Enterprise Server for Novell GroupWise is designed to use a trusted application key to open a connection to the GroupWise server. To generate the trusted application key, the GroupWise administrator runs the trusted application key generator, specifies the GroupWise primary domain database location, and then specifies the application name that the BlackBerry Enterprise Server should use to connect to the GroupWise server. The trusted application key is a 64-byte ASCII string. The BlackBerry Enterprise Server connects securely to a BlackBerry device user's mailbox using the trusted application name and key. The GroupWise server verifies the trusted application name and key and permits the BlackBerry Enterprise Server to establish a connection to the BlackBerry device user's GroupWise database.

Connections between the BlackBerry Desktop Manager and its components

The application loader tool and the media manager of the BlackBerry Desktop Manager share a secret password with the BlackBerry Desktop Manager. When the application loader tool or the media manager tool initiates a connection to the BlackBerry Desktop Software Version 4.2 or later, the BlackBerry Desktop Software uses secure channel technology to create a communication channel that is designed to use the shared secret password to secure communication between the BlackBerry Desktop Manager and either of those components.

Authentication process used by the secure channel technology communication channel

1. The application loader tool or the media manager tool initiates a connection to the BlackBerry Desktop Software Version 4.2 or later.

2. The BlackBerry Desktop Software implementation of the secure channel technology uses the shared secret password and the ECDH protocol with a 521-bit curve to create a master encryption key.
3. The secure channel technology uses the master encryption key to create two encryption keys and two HMAC-SHA-256 keys.
4. The secure channel technology uses one of the encryption keys and one of the HMAC keys to encrypt and authenticate data that the BlackBerry Desktop Software Version 4.2 sends over the communication channel to the components that store the same password.
5. The secure channel technology uses one of the encryption keys and one of the HMAC keys to encrypt and authenticate data that the BlackBerry Desktop Software Version 4.2 receives over the communication channel from the component that initiated the connection.

BlackBerry MDS connections

A BlackBerry device user can use the BlackBerry Browser and third-party Java applications on the BlackBerry device to access the Internet and your organization's intranet and to accept and respond to push requests from BlackBerry Enterprise Server push applications. The BlackBerry MDS uses standard Internet protocols such as HTTP and TCP/IP to access data on the Internet or your organization's intranet, and a RIM proprietary BlackBerry MDS Services security protocol to protect messages that the BlackBerry device sends using the BlackBerry MDS Services. The BlackBerry device uses standard BlackBerry encryption to protect your organization's applications and online and Internet data that a user receives on the BlackBerry device.

Requiring secure HTTP connections to the BlackBerry device

The BlackBerry MDS Services self-signed certificate permits server authentication between the BlackBerry MDS Services and the BlackBerry Manager, and client authentication between the BlackBerry MDS Services and external web services hosts. The BlackBerry MDS Services stores the self-signed certificate in its key store.

The system administrator can install the certificate on the BlackBerry MDS Services computer to establish server authenticated communication between the BlackBerry MDS Services and the BlackBerry Manager. If your BlackBerry Enterprise Solution uses SSL to communicate with external web servers, the system administrator must export the BlackBerry MDS Services certificate to those servers to establish authenticated communication with web services. If the BlackBerry Enterprise Server administrator uses the Weak Digest Algorithms IT policy rule to specify algorithms that BlackBerry devices consider weak, when BlackBerry devices use SSL to connect to external web servers, the BlackBerry Enterprise Server uses the list of weak digest algorithms when verifying that the certificate chains for the certificates that BlackBerry devices use with the SSL protocol are strong enough.

Using a secure connection to push BlackBerry MDS Studio Applications to BlackBerry devices

After the system administrator configures authentication between the BlackBerry MDS Services and web services, the BlackBerry Enterprise Server administrator can permit BlackBerry devices to install the BlackBerry® MDS Studio Applications that use SSL web services only.

Requiring secure HTTP connections using two-factor authentication

The BlackBerry MDS Services also support using RSA SecurID authentication with hardware tokens to require two-factor authentication when accessing the Internet or your organization's intranet on the BlackBerry device. When the user tries to access a web server, the BlackBerry MDS Connection Service checks whether it has cached credentials for the user. If it does, it sends the credentials to the web server. If it does not have cached credentials, or if the web server does not accept the cached credentials, the BlackBerry MDS Connection Service sends a message to the device that credentials are required, and the device prompts the user to type the credentials.

BlackBerry MDS Services security protocol

To authenticate the source and protect the integrity of each BlackBerry MDS message, the BlackBerry MDS Services security protocol generates a MAC for each BlackBerry MDS message that the BlackBerry device and the BlackBerry MDS Services send between them. To protect the confidentiality of each BlackBerry MDS

message, the BlackBerry MDS Services security protocol encrypts and decrypts data that the BlackBerry device and the BlackBerry MDS Services send between them.

Authentication process used by the BlackBerry MDS Services security protocol

1. The BlackBerry device generates the 128-bit AES session key.
2. The BlackBerry device uses 1024-bit RSA with PKCS #1 padding to encrypt the AES session key before sending it to the BlackBerry MDS Services server and storing it in the BlackBerry device flash memory.
3. The BlackBerry MDS Services security protocol uses 128-bit AES in CBC mode with PKCS #5 padding to encrypt a 128-bit AES session key using a 128-bit AES database access key.
4. The BlackBerry MDS Services server stores the encrypted 128-bit AES session key in the BlackBerry MDS Services database and stores the 128-bit AES database access key in the database key store.
5. The BlackBerry MDS Services security protocol uses HMAC with a SHA-1 hash function, in combination with the 128-bit shared secret key, to authenticate data that a BlackBerry device and the BlackBerry MDS Services send between them.
6. The BlackBerry MDS Services security protocol uses 128-bit AES in CBC mode with PKCS #5 padding to encrypt and decrypt data that a BlackBerry device and the BlackBerry MDS Services send between them.

Protecting the HTTP connection

If an application on the BlackBerry device accesses servers on the Internet, the BlackBerry Enterprise Server administrator can set up an HTTP connection that uses TLS/SSL, an HTTPS protocol, to provide additional authentication and security. The BlackBerry device supports HTTPS communication in the following modes:

HTTPS protocol	BlackBerry MDS encryption method	Description
proxy mode TLS/SSL	Sun® JSSE™ 1.4.1 cipher suite components	• The Connection Service sets up the proxy mode TLS/SSL connection on behalf of the BlackBerry device. • The BlackBerry device does not use proxy mode TLS/SSL to encrypt data traffic over the wireless network; standard BlackBerry encryption encrypts the data traffic between the BlackBerry device and BlackBerry Enterprise Server. Data traffic is therefore encrypted over the wireless network unless it is behind your organization's firewall. • The BlackBerry device experiences faster response times using this protocol than with handheld mode TLS/SSL.

HTTPS protocol	BlackBerry MDS encryption method	Description
Handheld mode TLS/SSL	TLS and WTLS key establishment algorithms, symmetric ciphers and hash algorithms that the RIM Crypto API currently supports on the BlackBerry device	• The BlackBerry device uses handheld (direct) mode TLS/SSL to encrypt data for the entire connection between the BlackBerry device and the content server. • Data traffic over the wireless network remains encrypted and is not decrypted at the Connection Service. • Use handheld mode TLS/SSL when only the endpoints of the transaction are trusted (for example, with banking services). **Note**: BlackBerry devices with BlackBerry Device Software Version 3.6.1 or later support BlackBerry device handheld mode TLS/SSL connections.

Using two-factor authentication to protect connections to enterprise Wi-Fi networks

The RSA SecurID Library on supported BlackBerry devices allows those BlackBerry devices to periodically generate software token tokencodes. The BlackBerry device combines the tokencode with a software token PIN that the BlackBerry device user provides as a prefix string to the tokencode to create a passcode for use with a two-factor authentication process on the BlackBerry device. When the BlackBerry device user tries to establish a WLAN or VPN connection that requires two-factor authentication on the BlackBerry device, the BlackBerry device prompts the BlackBerry device user to type the software token PIN and submit the current tokencode to create the two-factor authentication passcode.

How the BlackBerry device generates the software token for use with two-factor authentication

The BlackBerry device imports and uses random data called a seed to initialize the RSA SecurID software token algorithm. The algorithm generates the RSA SecurID software token tokencode on the BlackBerry device. When the BlackBerry device imports the .sdtid file seed into the RSA SecurID Library, the RSA SecurID Library randomly generates a password that the RSA SecurID Library uses to encrypt the .sdtid file seed

The RSA SecurID Library can decrypt the .sdtid file seed using an optional password if the administrator uses the RSA Authentication Manager Version 6.1 or later to set the password to issue an encrypted .sdtid file seed to the BlackBerry device user. The RSA SecurID Library uses code signing to prevent third party applications from altering or reading the information that it stores on the BlackBerry device.

For more information on how the BlackBerry device generates software token tokencodes, see "Appendix J: RSA SecurID software token tokencode generation process" on page 87.

How the BlackBerry Enterprise Solution authenticates requests for wireless software upgrades

The BlackBerry Enterprise Server and the BlackBerry device encrypt all communication between them, including wireless software upgrade communication, using standard BlackBerry encryption.

The BlackBerry device uses digital signature validation to authenticate the following types of wireless software upgrade communication:

- control messages that the BlackBerry device receives from the BlackBerry Infrastructure or the BlackBerry Provisioning System administration site that requests the wireless software upgrade
- upgrade instructions that the BlackBerry device requests and receives from the BlackBerry Infrastructure or the BlackBerry Provisioning System administration site sending the wireless BlackBerry Device Software upgrade

Authentication process for requests for wireless software upgrades

When the BlackBerry Infrastructure sends a wireless software upgrade communication, it performs the following actions:

1. Generates an ECDSA key periodically, using ECC over a 521-bit curve.
2. Signs the ECDSA key, using a stored root certificate.
3. Signs the wireless software upgrade communication that it sends to the BlackBerry device, using the digitally signed ECDSA key.

When the BlackBerry device receives the wireless software upgrade communication, it performs the following actions:

1. Verifies the ECDSA key, using a public key common to all BlackBerry devices that support wireless software upgrades.
2. Verifies the digital signature on the ECDSA key, using a stored root certificate.

WAP gateway connections

BlackBerry Device Software Version 3.2 SP1 or later supports WTLS, which is designed to provide an extra layer of security when connecting to a WAP gateway. WTLS requires a WAP gateway to provide standard WAP access to the Internet. To use a WAP gateway, your organization must work with the network operator or service provider.

Instant messaging server connections

The BlackBerry Collaboration Service is designed to provide a connection between the instant messaging server and enterprise instant messaging applications on BlackBerry devices. If your instant messaging server is Microsoft® Live Communications Server™, and if the enterprise messenger supported in your environment is BlackBerry® Instant Messaging for Microsoft® Windows Messenger, BlackBerry® Instant Messaging for Microsoft® Office Communicator, or both, the BlackBerry Enterprise Server administrator can change the transport protocol that the BlackBerry Collaboration Service uses to connect to the instant messaging server.

To provide additional authentication and security, the BlackBerry Enterprise Server administrator can require that the BlackBerry Collaboration Service uses TLS/SSL to connect to the instant messaging server. Using TLS/SSL might require that an instant messaging component has a digital certificate that binds the identity of that component to its public key. The instant messaging component can use its digital certificates to authenticate to another instant messaging component to allow encrypted communication between them.

If your environment is using Microsoft Windows Messenger, the BlackBerry Enterprise Server administrator can set the LCS Connector to use TLS to encrypt data that it sends to the Live Communications Server. The computer running the Microsoft Live Communications Server Connector must trust the TLS certificate on the Microsoft Live Communications Server. If the certificate that the Microsoft Live Communications Server uses is self-signed, the BlackBerry Enterprise Server administrator needs to install the certificate on the BlackBerry Collaboration Service computer.

If your environment is using Microsoft Office Communicator, the BlackBerry Enterprise Server administrator can set the BlackBerry Collaboration Service to use HTTPS to encrypt data that it sends to the Microsoft CWA Server. The Microsoft CWA Server and Microsoft Live Communications Server automatically encrypt data that they send between them using TLS.

Using segmented network architecture to prevent the spread of malware on your organization's network

The system administrator can separate your organization's network or LAN into multiple firewall-segmented components to create segmented network architecture. Each segment of your organization's network can contain network traffic, which improves the security and performance of the network segment by filtering out data that is not destined for that particular segment. If your organization's security policies enforce the use of

segmented network architecture, the system administrator can place the BlackBerry Enterprise Solution components in network segments.

To place the BlackBerry Enterprise Solution in multiple network segments, the system administrator must install each component on a remote computer and then place each computer in its own network segment. Placing the BlackBerry Enterprise Solution components in segmented network architecture is an option designed to prevent the spread of potential attacks from one BlackBerry Enterprise Solution component that exists on a remote computer to another computer within your organization's LAN. In a segmented network, attacks are isolated and contained on one computer. When each BlackBerry Enterprise Solution component resides in its own network segment, the system administrator allows remote communications by opening only the port connections that the BlackBerry Enterprise Solution components use.

For more information, see *Placing the BlackBerry Enterprise Solution in a Segmented Network*.

Preventing the spread of malware on your Wi-Fi network by using a network architecture that is segmented

If you have configured an enterprise Wi-Fi network that uses a VPN solution, when Wi-Fi enabled BlackBerry devices make connections to that network, they might allow the VPN concentrator, which acts as network gateway, to send data directly over port number 4101 to a BlackBerry Enterprise Server within the internal network of your organization. The VPN concentrator is the only device connected to the enterprise Wi-Fi network in this scenario. Configure your VPN concentrator to prevent it from opening unnecessary connections to the internal network.

Protecting Wi-Fi connections to the BlackBerry Enterprise Solution

If your wireless solution uses an enterprise Wi-Fi network to extend your organization's enterprise network, system administrators should protect the enterprise Wi-Fi network solution from unauthorized use, as they should protect the enterprise network. This protection should include the following requirements:

- all wireless client devices must complete authentication before gaining access to the network
- all wireless communications between wireless client devices and the network must be encrypted

The system administrator should make carefully considered security decisions for every enterprise Wi-Fi network installation. For details and recommendations, see your enterprise Wi-Fi network infrastructure component vendor(s).

Enterprise Wi-Fi network solution architecture security features

When the BlackBerry Enterprise Server administrator implements the BlackBerry Enterprise Solution over an enterprise Wi-Fi network, the BlackBerry Enterprise Server administrator must consider additional network security to protect all message and application data communication between the BlackBerry Enterprise Server and a supported Wi-Fi enabled BlackBerry device. Wi-Fi enabled BlackBerry devices are designed to reject incoming connections, to support limited connections in Wi-Fi infrastructure mode only, and to prevent Wi-Fi ad-hoc networking (peer-to-peer) connections.

Supported Wi-Fi enabled BlackBerry devices on an enterprise Wi-Fi network bypass the use of SRP by using the BlackBerry Router to send data between the BlackBerry Enterprise Server and the BlackBerry device. After the BlackBerry Router protocol establishes an authenticated connection successfully, the supported Wi-Fi enabled BlackBerry device uses a direct connection to the BlackBerry Enterprise Server using the BlackBerry Router instead of SRP connectivity and authentication. For more information about the BlackBerry Router protocol, see "BlackBerry Router protocol authentication" on page 39.

Standard BlackBerry encryption is designed to encrypt messages that the supported Wi-Fi enabled BlackBerry device and the BlackBerry Enterprise Server send between them after establishing an authenticated connection; supported Wi-Fi enabled BlackBerry devices also support multiple security methods that are designed to encrypt wireless communications over the enterprise Wi-Fi network between the BlackBerry device and wireless access points or a network firewall on the enterprise Wi-Fi network.

Accessing the BlackBerry Infrastructure

Wi-Fi enabled BlackBerry devices can connect directly to the BlackBerry Infrastructure over the Internet for access to voice and data services that a mobile network provider offers, even if UMA is not available. If a user's mobile network provider makes UMA technology (GAN technology) available, and the user has subscribed to the UMA feature, a Wi-Fi enabled BlackBerry device is designed to establish an IPSec VPN tunnel over the enterprise Wi-Fi network to the GANC automatically to access the mobile network provider's voice and data services.

The Wi-Fi enabled BlackBerry device and the BlackBerry Infrastructure send all data between them over the established SSL connection, which encrypts the data using a negotiable algorithm. For more information, see "Appendix I: Algorithm suites that the BlackBerry device supports for negotiating SSL connections" on page 85.

The BlackBerry Infrastructure sends its SSL certificate to the BlackBerry device when the BlackBerry device attempts to establish the SSL connection to the BlackBerry Infrastructure. The BlackBerry device uses a preloaded root certificate that is encrypted with a 1024 bit key to authenticate the SSL certificate. If the user deletes the root certificate on the BlackBerry device, when the BlackBerry device attempts to establish the SSL connection to the BlackBerry Infrastructure the device prompts the user to trust the SSL certificate.

Protecting connections from Wi-Fi enabled BlackBerry devices to the BlackBerry Infrastructure

A connection from a Wi-Fi enabled BlackBerry device to the BlackBerry Infrastructure over SSL is designed to provide the same protection that an SRP authenticated connection from the BlackBerry Enterprise Server to the BlackBerry Infrastructure provides. A user with malicious intent cannot use the connection to send data to or receive data from the BlackBerry device.

If a user with malicious intent tries to impersonate the BlackBerry Infrastructure, the BlackBerry device is designed to prevent the connection when the public key of the SSL certificate of the impersonated BlackBerry Infrastructure does not match the private key of the root certificate that is pre-installed on the BlackBerry device. If the BlackBerry device user accepts an invalid certificate, the connection cannot continue unless the BlackBerry device can use the connection to authenticate with a valid BlackBerry Enterprise Server or BlackBerry Internet Service.

Supported security features of Wi-Fi enabled BlackBerry devices

Wi-Fi enabled BlackBerry devices are designed to operate on supported IEEE 802.11 enterprise Wi-Fi networks to let on-site BlackBerry device users access email, organizer, and browser-based applications over the wireless network while those BlackBerry device users are mobile in the physical environment of their organization. Wi-Fi enabled BlackBerry devices provide enterprise Wi-Fi network configuration options that are designed to be compatible with the wireless security policies and environments of most organizations, and use the security features of the BlackBerry Enterprise Solution.

Wi-Fi enabled BlackBerry devices support the following categories of enterprise Wi-Fi network security technology:

Enterprise Wi-Fi network security technology	Wi-Fi enabled BlackBerry device implementation
Enterprise captive portal	Set authentication with enterprise captive portals (enterprise Wi-Fi networks outside of your organization's network) using a configured login web page.

Enterprise Wi-Fi network security technology	Wi-Fi enabled BlackBerry device implementation
Layer 2 security	Set layer 2 (the IEEE® 802.11® link layer) security methods and protocols for use with layer 2 methods that operate between the BlackBerry device and a wireless access point on the enterprise Wi-Fi network using encryption, or encryption and BlackBerry device user authentication. The BlackBerry device supports the following layer 2 security methods: • open (no security method) • 64-bit and 128-bit WEP encryption • PSK • IEEE 802.1x and EAP authentication framework support (RFC 3748) using LEAP, PEAP, EAP-TTLS, EAP-FAST, EAP-SIM, and EAP-TLS (RFC 2716) The BlackBerry device supports the use of TKIP and AES-CCMP encryption for WPA™-Personal, WPA2™-Personal, WPA-Enterprise, and WPA2-Enterprise.
Layer 3 security	Use VPNs (the only layer 3 security method that the BlackBerry device currently supports) at the IP layer.
Two-factor authentication	Use passcodes to authenticate the BlackBerry device user to enterprise Wi-Fi networks using PEAP, EAP-FAST and EAP-TTLS authentication methods and VPNs. The BlackBerry device supports using automatic PAC provisioning with EAP-FAST only.

For more information about the security methods and encryption algorithms that the BlackBerry device supports, see "Appendix H: Enterprise Wi-Fi security methods that the BlackBerry device supports" on page 82.

IEEE 802.1X environment components

An IEEE 802.1X environment includes the following components:

- IEEE 802.1X/EAP client software, also called a supplicant, running on the enterprise Wi-Fi network client device

  The Wi-Fi enabled BlackBerry device has a built-in IEEE 802.1x supplicant.
- IEEE 802.1x software running on the access point, also called an authenticator
- authentication server that authenticates the enterprise Wi-Fi network client device on behalf of the authenticator and allows the Wi-Fi network client to authenticate the Wi-Fi network

  In most cases, the authentication server uses the RADIUS protocol (RFC 2865 and RFC 3579) to communicate with the authenticator on the access point.

How the IEEE 802.1x environment controls access to the enterprise Wi-Fi network

When a wireless client first associates itself with an access point that is enabled for IEEE 802.1x security, the only communication that that access point permits is IEEE 802.1x authentication. Using a negotiated EAP method, the supplicant on the supported Wi-Fi enabled BlackBerry device sends its credentials (typically, a BlackBerry device user name and password) to the access point, which forwards the information to the authentication server. The authentication server authenticates the supported Wi-Fi enabled BlackBerry device on behalf of the access point and instructs the access point to permit or prevent access to the enterprise Wi-Fi network. The authentication server sends Wi-Fi network credentials to the supported Wi-Fi enabled BlackBerry device to allow it to authenticate the access point.

After an authentication server permits the supported Wi-Fi enabled BlackBerry device to access the enterprise Wi-Fi network, the access point and the BlackBerry device use IEEE 802.1x EAPoL-Key messages to establish the WEP, TKIP, or AES-CCMP encryption keys, depending on the EAP method that is set on the BlackBerry device. After the access point and the supported Wi-Fi enabled BlackBerry device establish encryption keys, the BlackBerry device has encrypted access to the enterprise Wi-Fi network.

If your enterprise Wi-Fi solution is using one of the supported EAP authentication methods, all of which are designed to provide mutual authentication between supported Wi-Fi enabled BlackBerry devices and the enterprise Wi-Fi network, the BlackBerry Enterprise Server administrator can grant and revoke supported Wi-Fi enabled BlackBerry devices access to the enterprise Wi-Fi network by updating the central authentication server only. The system administrator does not need to update the configuration of each access point.

Administering enterprise Wi-Fi network solution security using IT policy rules

With the BlackBerry Enterprise Solution, the BlackBerry Enterprise Server administrator can monitor and control all BlackBerry devices from the BlackBerry Manager using wireless IT commands and IT policy rules. The enterprise Wi-Fi network solution includes specific IT policy rules for the security of the enterprise Wi-Fi network solution. The BlackBerry Enterprise Server administrator can turn Wi-Fi access on and off on supported Wi-Fi enabled BlackBerry devices on BlackBerry Enterprise Server Version 4.1 SP3 or later, and manage WLAN and VPN settings for individual user accounts on BlackBerry Enterprise Server Version 4.1 SP2 or later.

For more information about using VPN and WLAN IT policy rules and setting configuration profiles to configure your enterprise Wi-Fi network solution to support Wi-Fi enabled BlackBerry devices, see the *BlackBerry Enterprise Server Wi-Fi Implementation Supplement*.

Requiring protected connections to enterprise Wi-Fi networks

Using WEP encryption to protect connections to enterprise Wi-Fi networks

WEP, the oldest, most prevalent form of enterprise Wi-Fi network encryption available, was originally designed to bring the same level of security to an enterprise Wi-Fi network as is available on a traditional wired LAN. WEP uses a matching encryption key at both the access point and the wireless client to secure wireless communication. This key can be 40 bits (for 64-bit WEP) or 104 bits (for 128-bit WEP) in length.

To use WEP, the BlackBerry Enterprise Server administrator must distribute WEP keys to the supported Wi-Fi enabled devices on your enterprise Wi-Fi network. In the BlackBerry Manager, the BlackBerry Enterprise Server administrator can define WEP keys for each supported Wi-Fi enabled device using IT policy rules set in an IT policy that the BlackBerry Enterprise Server sends to the supported Wi-Fi enabled device when the BlackBerry Enterprise Server activates and registers the supported Wi-Fi enabled device and whenever the BlackBerry Enterprise Server administrator updates the IT policy thereafter.

By current industry standards, WEP is not a cryptographically strong security solution. Identified WEP weaknesses include the following scenarios:

- an attacker could capture transmissions over the wireless network and might thereby be able to deduce WEP keys in very little time
- an attacker might be able to use an undetected man-in-the-middle attack to alter WEP-encrypted packets

Organizations that use WEP as their preliminary security method to moderately limit access to their enterprise Wi-Fi network might also use a VPN to provide data confidentiality by authenticating and encrypting access to their core enterprise network, if they are concerned about security.

Using IEEE 802.11i to protect connections to enterprise Wi-Fi networks

IEEE 802.11i defines an enhanced security protocol to protect Wi-Fi networks. It uses the IEEE 802.1X standard for authentication and key management. The IEEE 802.1x standard defines a generic authentication framework that enterprise Wi-Fi network client devices and wired or wireless networks can use to authenticate with each other to permit or prevent the enterprise Wi-Fi network client devices accessing the network. IEEE 802.11i specifies two Wi-Fi network access control methods: one based on PSKs and one based on IEEE 802.1x, which uses EAP protocols for authentication.

Authentication method	Description	Wi-Fi enabled BlackBerry device implementation
Using IEEE 802.11i with PSK	Small office and home environments where it is not feasible to set up a server-based authentication infrastructure might use IEEE 802.1x with the PSK method. The access point and the wireless client use a PSK (also known as a passphrase) to mutually derive link layer encryption keys. The PSK method uses TKIP or AES-CCMP algorithms to secure enterprise Wi-Fi network communications, but it relies on a single, shared passphrase of up to 256 bits in length for access control. All access points and wireless clients must know the passphrase.	The supported Wi-Fi enabled BlackBerry device implementation of PSK is compatible with the WPA-Personal and WPA2-Personal specifications. The BlackBerry Enterprise Server administrator can set the passphrase and distribute it to the supported Wi-Fi enabled BlackBerry device using the WLAN Preshared Key IT policy rule.
Using the IEEE 802.11i with IEEE 802.1X authentication	An IEEE 802.1x framework can use EAP methods to provide authentication. LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, and EAP-FAST authentication methods are designed to provide mutual authentication between the supported Wi-Fi enabled BlackBerry device and the enterprise Wi-Fi network.	To act as a WLAN supplicant device, the supported Wi-Fi enabled BlackBerry device implements WLAN authentication processes that use EAP methods as specified in RFC 3748 and meet the requirements of RFC 4017. Supported Wi-Fi enabled BlackBerry devices are designed to use EAP methods (EAP-TLS, EAP-TTLS, EAP-FAST, and PEAP) to mutually authenticate to WLAN networks, as specified in the WPA™-Enterprise and WPA2™-Enterprise specification, which use credentials to provide mutual authentication: When the supported Wi-Fi enabled BlackBerry device sends EAPoL messages, it uses the encryption and message integrity protection specified by the EAP method. When the BlackBerry device transmits EAPoL-Key messages it uses either RC4 or AES algorithms to provide message integrity and encryption.

Using certificate-based authentication to protect connections to enterprise Wi-Fi networks

If the BlackBerry Enterprise Server administrator uses PEAP, EAP-TLS, or EAP-TTLS methods to secure the access points on your enterprise Wi-Fi network, supported Wi-Fi enabled BlackBerry devices must mutually authenticate with an access point through an authentication server to connect to the enterprise Wi-Fi network. The BlackBerry Enterprise Server administrator requires a certificate authority server to generate the certificates that the supported Wi-Fi enabled BlackBerry devices and the RADIUS server will store.

Successful PEAP, EAP-TLS, or EAP-TTLS authentication requires that the supported Wi-Fi enabled BlackBerry devices trust the certificate of the access authentication server. The certificate binds the authentication server identity to a public and private key pair. Supported Wi-Fi enabled BlackBerry devices do not automatically trust

the authentication server certificate. For the supported Wi-Fi enabled BlackBerry devices to trust the authentication server certificates, the following conditions must exist:

- a certificate authority server that the supported Wi-Fi enabled BlackBerry devices and the authentication server mutually trust must generate the certificate for the authentication server and the certificate for each supported Wi-Fi enabled BlackBerry device
- the root certificate(s) in the certificate chain to which the certificate of the authentication server belongs must exist on supported Wi-Fi enabled BlackBerry devices that use PEAP, EAP-TLS, or EAP-TTLS

Each BlackBerry device stores a list of explicitly trusted root certificates that certificate authorities have issued.

Caching connection information when using IEEE 802.1X authentication

When using IEEE 802.11i with IEEE 802.1X authentication, the supported Wi-Fi enabled BlackBerry device and the access point can cache a PMK, which is derived from keying material that the EAP exchange generates. PMK caching reuses previously established keying material to skip IEEE 802.1x authentication and mutually derive session keys with an access point to which it is connecting. Use this feature to help reduce the roaming latency between access points in an enterprise Wi-Fi network environment for the supported Wi-Fi enabled BlackBerry device.

Using VPNs to protect connections to enterprise Wi-Fi networks

Your organization might use VPNs, including IPSec VPNs, to provide remote BlackBerry device users with secure access to an enterprise network. A VPN provides a strongly encrypted tunnel between the client device and the core enterprise network. A VPN differs from the other supported enterprise Wi-Fi network security methods in that the access point is not involved in data encryption.

An enterprise Wi-Fi VPN solution consists of the following components:

- a VPN client on the supported Wi-Fi enabled BlackBerry device which the BlackBerry device uses to gain access to the network
- a VPN concentrator, which is located on the edge of your organization's enterprise network and acts as the gateway to that network

When your organization uses a VPN to protect access to the enterprise Wi-Fi network, the enterprise Wi-Fi network configuration also uses a Wi-Fi authentication or encryption method by default to provide an access-control mechanism for the enterprise Wi-Fi network itself, and uses VPN to provide the actual secure access method. In this scenario, the enterprise Wi-Fi network is configured as an untrusted network, and the VPN concentrator is the only device connected to the enterprise Wi-Fi network.

The VPN client on a supported Wi-Fi enabled BlackBerry device is designed to

- use strong encryption to authenticate itself with the VPN concentrator
- create an encrypted tunnel between the supported Wi-Fi enabled BlackBerry device and the VPN concentrator through which the supported Wi-Fi enabled BlackBerry device and the enterprise network can route all communication between them

Using enterprise captive portals to protect connections to enterprise Wi-Fi networks or Wi-Fi hotspots

A captive portal is a web-based authentication mechanism to permit access to an enterprise Wi-Fi network or Wi-Fi hotspot. Supported Wi-Fi enabled BlackBerry devices can use a captive portal to gain access to an IP filtered segment of the enterprise Wi-Fi network or hotspot. After using a captive portal to connect to an enterprise network or hotspot, the user can send a browser request for a website from the supported Wi-Fi enabled BlackBerry device to an HTML login page, which allows the enterprise Wi-Fi network or hotspot to authenticate the BlackBerry device before permitting it access to the website.

If your organization has an enterprise captive portal, the BlackBerry Enterprise Server administrator can permit users to access the captive portal using the WLAN Login application on the BlackBerry device. BlackBerry device

users must authenticate with the WLAN Login application browser using login credentials that the system administrator provides.

When the BlackBerry device authenticates with the captive portal, the BlackBerry device user can use the BlackBerry® Browser on the BlackBerry device to access other web sites and data service available on the segregated Wi-Fi network. The BlackBerry device is designed to support web browsing using the BlackBerry MDS Connection Service.

Authenticating a BlackBerry device user

When a user receives a new BlackBerry device, the BlackBerry Enterprise Solution uses either a desktop based or wireless master encryption key generation method to authenticate the user and the BlackBerry device to the BlackBerry Enterprise Server. The BlackBerry device user must have a valid email address for the BlackBerry device to activate successfully and register with the wireless network.

Authenticating a user to a BlackBerry device using a password

When the BlackBerry Enterprise Server administrator adds a BlackBerry device to a BlackBerry Enterprise Server, the BlackBerry Enterprise Server administrator can require a BlackBerry device user to authenticate to the BlackBerry device using a security password. The BlackBerry Enterprise Server administrator can use IT policy rules to set features such as password duration, length, and strength, to require password patterns, and to forbid specific passwords. For more information, see the *Policy Reference Guide*.

If the BlackBerry device user intends to activate the BlackBerry device over the wireless network, they must contact the BlackBerry Enterprise Server administrator for a temporary activation password that the BlackBerry device uses to establish the master encryption key. The BlackBerry Enterprise Server administrator can set the BlackBerry device activation password and communicate it to the BlackBerry device user.

The activation password

- applies to that BlackBerry device user's email account only
- is not valid after five unsuccessful activation attempts
- expires if the BlackBerry device user does not activate the BlackBerry device within the default period of 48 hours, or a period of up to 720 hours that the BlackBerry Enterprise Server administrator sets after creating the activation password
- is deleted from the BlackBerry Enterprise Server when the BlackBerry device activates successfully

Authenticating a BlackBerry device user using a smart card

Use two-factor authentication, using a smart card, to require BlackBerry device users to prove their identities to their BlackBerry device using two factors:

- what they have (the smart card)
- what they know (their smart card password).

The BlackBerry Smart Card Reader integrates smart card use with the BlackBerry Enterprise Solution, enabling BlackBerry device users to authenticate with their smart cards to login to certain Bluetooth enabled BlackBerry devices.

The BlackBerry Smart Card Reader

- creates a reliable two-factor authentication environment for granting BlackBerry device users access to BlackBerry and PKI applications
- is designed to enable the wireless digital signing and encryption of wireless email messages using the S/MIME Support Package for BlackBerry devices
- stores all encryption keys in RAM only and never writes the keys to flash memory

For more information, see the *BlackBerry Smart Card Reader Security Technical Overview*.

Binding the smart card to the BlackBerry device

If a user has a smart card authenticator, smart card driver, and smart card reader driver installed on their BlackBerry device, either the BlackBerry Enterprise Server administrator or that user can initiate two-factor authentication on the BlackBerry device to bind the BlackBerry device to the installed smart card. After the BlackBerry device binds to the smart card, it requires that smart card to authenticate the user.

The BlackBerry Enterprise Server administrator can set the Force Smart Card Two-Factor Authentication IT policy rule in the BlackBerry Manager to require that a user authenticates with the BlackBerry device using a smart card. If the BlackBerry Enterprise Server administrator does not force the user to authenticate with the BlackBerry device using a smart card, the user can turn two-factor authentication on and off with their smart card by setting the User Authenticator field in the BlackBerry device Security Options.

When the BlackBerry Enterprise Server administrator or the user enables two-factor authentication, the following events occur:

1. The BlackBerry device locks.
2. When a user tries to unlock the BlackBerry device, the BlackBerry device prompts the user to type the BlackBerry device password. If the user has not yet set a BlackBerry device password, the BlackBerry device forces them to set one.
3. The BlackBerry device prompts the user to type the user authenticator (smart card) password to turn on two-factor authentication with the installed smart card.
4. The BlackBerry device binds to the installed smart card automatically by storing the following smart card binding information in a special BlackBerry device NV store location that is inaccessible to a user:
   - the name of a Java class that the BlackBerry Smart Card Reader requires
   - the binding information format
   - the smart card type

   Note: For the Common Access Card, this string is "GSA CAC".
   - the name of a Java class that the smart card code requires
   - a unique 64-bit identifier that the smart card provides
   - a smart card label that the smart card provides (for example, "GRAHAM.JOHN.1234567890")
5. The BlackBerry device pushes the current IT policy to the BlackBerry Smart Card Reader.

Confirming that the BlackBerry device is bound to the correct smart card

After a user turns on two-factor authentication, whenever the BlackBerry device prompts the user to insert the smart card into the BlackBerry Smart Card Reader, the BlackBerry device prompt indicates the label and the card type of the correct (bound) smart card. If the BlackBerry device is running BlackBerry Device Software Version 3.6 with either the S/MIME Support Package Version 1.5 for BlackBerry devices installed or no S/MIME Support Package for BlackBerry devices installed, the information in the prompt is the only indication that a smart card is bound to the BlackBerry device.

If the BlackBerry device is running BlackBerry Device Software Version 4.0 or later (S/MIME Support Package for BlackBerry devices optional), the user can also view smart card information in the BlackBerry device Security Options.

Field	Description
Name	indicates the type of the installed smart card

Field	Description
Initialized	indicates whether the BlackBerry device is authenticated with and bound to the smart card • a value of Yes indicates that the BlackBerry device is bound to the smart card • a value of No indicates that the BlackBerry device is not bound to the smart card

Controlling BlackBerry devices

With the BlackBerry Enterprise Solution, the BlackBerry Enterprise Server administrator can monitor and control all BlackBerry devices over the wireless network from the BlackBerry Manager.

Controlling BlackBerry device behavior using IT policy rules

Use one or more IT policies to control the behavior of BlackBerry devices and the BlackBerry Desktop Software in your organization.

The Default IT policy includes all standard IT policy rules on the BlackBerry Enterprise Server. When new users in a BlackBerry Domain complete activation of their BlackBerry devices on the BlackBerry Enterprise Server, the BlackBerry Enterprise Server automatically pushes the Default IT policy to their BlackBerry devices. The BlackBerry Enterprise Server administrator can use either of the following methods to change the default behavior of BlackBerry devices and BlackBerry Desktop Software in your organization:

- set the values of IT policy rules in the Default IT policy
- create a new IT policy, set its IT policy rule values, and assign one or more users or user groups to the new IT policy

Changing the default behavior

An IT policy rule enables the BlackBerry Enterprise Server administrator to customize and control BlackBerry device and BlackBerry Desktop Software functionality using the following methods:

- setting an IT policy rule to a True or False value
- typing a string, which simultaneously turns on an IT policy rule and provides the parameters for its use
- selecting a predefined permitted value to assign to an IT policy rule

The BlackBerry Enterprise Server administrator cannot use all IT policy rules to set the behavior of all BlackBerry device types. For more information, see the *Policy Reference Guide*.

The BlackBerry Manager groups the IT policy rules by common properties or by application. Most IT policy rules are intended to be assigned to more than one BlackBerry device. Some IT policy rules set a unique value and are intended to be assigned to one BlackBerry device and one user only. For more information on those IT policy rules, see the *BlackBerry Enterprise Server Implementation Guide for Wireless LAN*.

Reverting to the default behavior

To revert to the default behavior that an IT policy rule customizes or controls, the BlackBerry Enterprise Server administrator can set that IT policy rule to Default, if that setting is available, or delete the previously set value.

If the BlackBerry Enterprise Server administrator assigns users to a new IT policy, the BlackBerry Enterprise Server administrator can delete that IT policy to revert those users to the default behavior for all functionality on the BlackBerry device and the BlackBerry Desktop Software. The BlackBerry Enterprise Server automatically reassigns the users to the Default IT policy and resends the Default IT policy to the BlackBerry device, enforcing the default settings. The BlackBerry Enterprise Server administrator cannot delete the Default IT policy.

Creating new IT policy rules to control custom applications

Create new IT policy rules to control custom applications that your organization develops to run in BlackBerry environments. After the BlackBerry Enterprise Server administrator creates a new IT policy rule, the BlackBerry Enterprise Server administrator can add it to and assign a value to it in any new or existing IT policy. Only your organization's own custom applications can use new IT policy rules that the BlackBerry Enterprise Server administrator creates. The BlackBerry Enterprise Server administrator cannot create new IT policy rules to control standard BlackBerry device functionality.

Enforcing IT policy changes over the wireless network

Wireless IT policy enables the BlackBerry Enterprise Server administrator to immediately enforce IT policy rule additions, deletions, or modifications on C++ enabled BlackBerry devices running BlackBerry Device Software Version 2.5 or later and on Java enabled BlackBerry devices running BlackBerry Device Software Version 3.6 or later. When the BlackBerry device receives an updated Default IT policy or a new IT policy, the BlackBerry device and BlackBerry Desktop Software apply the configuration changes.

The BlackBerry Enterprise Server must resend the IT policy to the BlackBerry device to update the BlackBerry device and the BlackBerry Desktop Software behavior over the wireless network. By default, the BlackBerry Enterprise Server is designed to resend the IT policy to BlackBerry devices of users that are assigned to that IT policy within a short period of time after the BlackBerry Enterprise Server administrator updates the IT policy.

The BlackBerry Enterprise Server administrator can also resend an IT policy to the user account of a specific BlackBerry device manually, and the BlackBerry Enterprise Server administrator can set the BlackBerry Enterprise Server to resend IT policies to BlackBerry devices on that specific BlackBerry Enterprise Server at a scheduled interval whether or not the BlackBerry Enterprise Server administrator has changed the IT policies.

Enforcing BlackBerry device and BlackBerry Desktop Software security

The BlackBerry Enterprise Solution offers a user many different security settings for the BlackBerry device and BlackBerry Desktop Software. For example, the BlackBerry Enterprise Server administrator can specify one or more IT policy rules to enforce the following behavior to meet your organization's security requirements:

- Enforce encryption (for example, encryption of user data and messages that the BlackBerry Enterprise Server forwards to the message recipient) and encryption strength
- Enforce password or passphrase use
- Enforce a strong password or passphrase
- Secure Bluetooth connections
- Protect user data on the BlackBerry device
- Protect master encryption keys on the BlackBerry device
- Restrict application use on the BlackBerry device
- Restrict BlackBerry device resources available to third-party applications

For more information, see the *Policy Reference Guide*.

Controlling BlackBerry device access to the BlackBerry Enterprise Server

Turn on the Enterprise Service Policy to control which BlackBerry devices can connect to the BlackBerry Enterprise Server. After the BlackBerry Enterprise Server administrator turns on the Enterprise Service Policy, the BlackBerry Enterprise Server still permits connections from BlackBerry devices and BlackBerry enabled devices that the BlackBerry Enterprise Server administrator previously added to the BlackBerry Enterprise Server, but it prevents connections from newly-added BlackBerry devices by default.

Define BlackBerry device criteria in an approval list to turn on and turn off BlackBerry Enterprise Server access for BlackBerry devices. BlackBerry devices that meet the approval list criteria can complete wireless enterprise activation on that BlackBerry Enterprise Server.

The BlackBerry Enterprise Server administrator can define the following types of criteria:

- specific, permitted BlackBerry device PINs as a string
- a permitted range of BlackBerry device PINs

The BlackBerry Enterprise Server administrator can also control access based on specific manufacturers and models of BlackBerry devices. The BlackBerry Manager includes lists of permitted manufacturers and models based on the properties of BlackBerry devices already added to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server administrator can uncheck items on these lists to prevent further connections from BlackBerry devices of a specific manufacturer or model.

The BlackBerry Enterprise Server administrator can permit a specific user to override the Enterprise Service Policy. If the BlackBerry Enterprise Server administrator then sets the approval list with criteria that excludes that user's BlackBerry device or BlackBerry enabled device, the user can still connect to the BlackBerry Enterprise Server.

For more information, see the *BlackBerry Enterprise Server System Administration Guide*.

Controlling wireless software upgrades using the BlackBerry Enterprise Server

By default, only the BlackBerry Enterprise Server can select available wireless software upgrade packages and send them to BlackBerry devices to request that BlackBerry devices upgrade to the software packages. The wireless service provider cannot select available BlackBerry Device Software upgrade packages and send them to BlackBerry devices unless you set the BES Upgrade Exclusivity flag in the OTASL IT Policy Flags IT policy rule to turn off exclusive BlackBerry Enterprise Server control of wireless software upgrade requests.

Protecting Bluetooth connections on BlackBerry devices

Bluetooth wireless technology enables Bluetooth enabled BlackBerry devices to establish a wireless connection with devices that are within a 10-meter range. Bluetooth enabled BlackBerry devices can connect to other Bluetooth enabled devices such as a hands-free car kit or wireless headset.

Bluetooth profiles specify how applications on Bluetooth enabled BlackBerry devices and on other Bluetooth devices connect and interoperate. Bluetooth enabled BlackBerry devices implement their Bluetooth serial port profiles to establish serial connections to Bluetooth peripherals using virtual serial ports. The Bluetooth software on the BlackBerry device accesses the serial port through the BlackBerry Software Development Kit.

The BlackBerry Enterprise Server administrator can use IT policies to simultaneously manage all Bluetooth enabled BlackBerry devices. By default, Bluetooth enabled BlackBerry devices that are running BlackBerry Device Software Version 4.0 or later include the following security measures:

- The Bluetooth wireless technology is turned off on the BlackBerry device.
- Users must request a connection or pairing on the BlackBerry device with another Bluetooth device. Users must also type a shared secret key (called a passkey) to complete the pairing.
- Users can specify whether to encrypt data traffic to and from the BlackBerry device over Bluetooth connections. The BlackBerry Enterprise Solution uses the passkey to generate encryption keys.
- The BlackBerry device prompts the user each time a Bluetooth device attempts to connect to the BlackBerry device.

For more information, see *Security for BlackBerry Devices with Bluetooth Wireless Technology*.

Using Bluetooth CHAP password authorization on the BlackBerry device

Supported Bluetooth enabled BlackBerry devices support using CHAP as described in RFC 1994. CHAP is a protocol designed to authenticate the client using a challenge that is combined with a secret (for example, the BlackBerry device password).

BlackBerry devices that support and are enabled to use CHAP can use it to establish a Bluetooth link to the BlackBerry Desktop Software so that the BlackBerry device never sends its password over an unprotected

connection. BlackBerry devices and the BlackBerry Desktop Software can use CHAP to send a challenge and subsequently use the SHA-1 algorithm to either calculate a response to the challenge or validate the response of the other party, depending on which party initiated the Bluetooth link establishment process.

Controlling location-based services on the BlackBerry device

Third-party applications and preloaded BlackBerry applications on BlackBerry devices that support the GPS feature can use the GPS feature by default. For example, BlackBerry® Maps is a preloaded application that uses the GPS feature on BlackBerry devices to enable users to locate the global positions of their BlackBerry devices. The BlackBerry Enterprise Server includes the following options to enable the BlackBerry Enterprise Server administrator to control the GPS feature and the location-based services on supported BlackBerry devices that use the feature.

Option	Description
Turn off the GPS feature on BlackBerry devices.	The following measures prevent third-party applications and preloaded BlackBerry applications from accessing the global position of the BlackBerry device: • The BlackBerry Enterprise Server administrator can set the Disable GPS IT policy rule to True to prevent the BlackBerry device from permitting third-party applications or preloaded BlackBerry applications from accessing the GPS feature. • The BlackBerry Enterprise Server administrator can set the Device GPS application control policy rule to Not Permitted in the default application control policy to prevent all third-party applications from using the GPS feature.
Control use of the GPS feature by specific third-party applications on the BlackBerry device.	The BlackBerry Enterprise Server administrator can set the Device GPS application control policy rule to Not Permitted in a specific application control policy to prevent specific third-party applications from using the GPS feature.
Prevent the BlackBerry device from reporting its location to the BlackBerry Enterprise Server.	By default, the Enable Enterprise Location Tracking IT policy rule is set to False to prevent the BlackBerry device from using the GPS feature to report its location to the BlackBerry Enterprise Server at regular intervals. The BlackBerry Enterprise Server administrator can turn on Enterprise Location Tracking, specify a message that the BlackBerry device displays to notify the BlackBerry device user when Enterprise Location Tracking is enabled, and configure the interval after which a BlackBerry device reports its location to the BlackBerry Enterprise Server.
Turn off the BlackBerry Maps application on BlackBerry devices.	The BlackBerry Enterprise Server administrator can use the Disable BlackBerry Maps IT policy rule to specify whether the BlackBerry Maps application is turned off on the BlackBerry device.

How the BlackBerry device protects its operating system and the BlackBerry Device Software

Each time a user turns on the BlackBerry device specific components on the BlackBerry device automatically check the authenticity of the operating system and the integrity of the BlackBerry Device Software. The BlackBerry Device Software must pass these security tests before users can run the software on the BlackBerry device and wireless software upgrades can update the software successfully.

Protecting the BlackBerry device against malware

Java based BlackBerry devices are designed to provide an open platform for third-party wireless enterprise application development. Using BlackBerry MDS Studio and the BlackBerry® Java® Development Environment (BlackBerry JDE), the BlackBerry Enterprise Solution lets software developers create third-party applications for BlackBerry devices. BlackBerry JDE developers can create more powerful, sophisticated applications than are possible with the standard Java 2 Platform, Micro Edition (J2ME™). A third-party BlackBerry application can perform the following tasks on the BlackBerry device:

- communicate and share persistent storage with other third-party BlackBerry applications
- interact with native BlackBerry applications
- access user data such as calendar entries, email messages, and contacts

Third-party applications that are designed with malicious intent to cause harm to computer systems (for example, viruses, trojans, worms and spyware) are commonly known, collectively, as malware. Some malware attacks could target BlackBerry devices. Attackers could use malware to perform attacks that are designed to

- steal your personal data and your organization's data
- create a DoS to make your network unusable
- access your organization's network using your organization's BlackBerry devices

By default, Java based BlackBerry devices can download any third-party application over the wireless network using the BlackBerry Browser. The BlackBerry Enterprise Server administrator can also send third-party applications to BlackBerry devices over the wireless network, and install them on BlackBerry devices automatically. The BlackBerry Enterprise Solution includes tools designed to enable the BlackBerry Enterprise Server administrator to control the manual or automatic installation of third-party applications and limit the access of untrusted applications to the BlackBerry device and its resources to help contain malware attacks on the BlackBerry device.

On computers, malware prevention requires processes that both detect and contain malware attacks. Detection is the process of determining whether or not an application is malware. Effective malware detection requires a comprehensive and frequently-updated local database or a constant connection to a similarly qualified online database. While computers might have access to these databases, current mobile devices do not have enough storage space for a malware database and cannot guarantee a constant connection to the Internet.

The BlackBerry Enterprise Solution is designed to use IT policies, application control policies, and code signing to contain malware by controlling third-party application access to the BlackBerry device resources and applications. These containment methods are designed to prevent malware that might gain access to the BlackBerry device from causing damage to the BlackBerry device, its applications and its data, or your organization's network.

For more information, see *Protecting the BlackBerry device platform against malware*.

Using IT policy rules to contain malware on the BlackBerry device

The BlackBerry Enterprise Server Version 4.1 SP2 or later includes IT policy rules that are designed to enable the BlackBerry Enterprise Server administrator to

- prevent BlackBerry devices from downloading third-party applications over the wireless network

- specify whether or not applications, including third-party applications, on the BlackBerry device can initiate specific types of connections

Note: The BlackBerry Enterprise Server administrator cannot use an IT policy to permit or prevent downloading specific applications on the BlackBerry device. The BlackBerry Enterprise Server administrator can do this using one or more application control policies.

Using application control policy rules to contain malware on the BlackBerry device

The BlackBerry Enterprise Server application control policy rules are designed to let the BlackBerry Enterprise Server administrator allow or prevent the installation of specific third-party applications on the BlackBerry device and to limit the permissions of third-party applications, including

- the resources (for example, email, phone, and BlackBerry device key store) that third-party applications can access on the BlackBerry device
- the types of connections that a third-party application running on the BlackBerry device can establish (for example, local, internal, and external connections)
- whether or not an application can access the user authenticator framework API, which permits the registration of drivers to provide two-factor authentication to unlock the BlackBerry device

For example, to control connections to your internal servers from third-party applications on the BlackBerry device, the BlackBerry Enterprise Server administrator can create an application control policy that prevents the application to which it is assigned from making internal connections. When the BlackBerry Enterprise Server administrator applies the application control policy to a software configuration for a user or one or more user groups, those BlackBerry device users might not be able to use the full functionality of any third-party application to which the BlackBerry Enterprise Server administrator assigns the application control policy to send and receive data from internal servers. When the BlackBerry Enterprise Server administrator sets application policy rules for user groups, the BlackBerry Enterprise Server limits allowed application behavior to a small subset of trusted BlackBerry device users only.

IT policy rule settings override application control policy rule settings. For example, if the BlackBerry Enterprise Server administrator changes the Allow Internal Connections IT policy rule setting (the default value is True) for BlackBerry devices for which the BlackBerry Enterprise Server administrator also sets an application control policy that allows a specific application to make internal connections, the IT policy rule setting overrides the application control policy rule setting and the application cannot make internal connections.

The BlackBerry device resets if the permissions of the application to which it is applied become more restrictive. BlackBerry devices running BlackBerry Device Software Version 4.1 or later permit users to make application permissions more, but never less restrictive than what is set by the BlackBerry Enterprise Server administrator.

Using code signing to contain malware on the BlackBerry device

RIM does not inspect or verify third-party applications that run on BlackBerry devices; however, RIM controls the use of BlackBerry device APIs that include sensitive packages, classes, or methods to prevent unauthorized applications from accessing data on the BlackBerry device. Each third-party application requires authorization to run on the BlackBerry device.

Before the BlackBerry Enterprise Server administrator or a BlackBerry device user can run a third-party application that uses the RIM controlled APIs on the BlackBerry device, the RIM signing authority system must use public key cryptography to authorize and authenticate the application code. The third-party application developer must visit www.blackberry.com/developers/downloads/jde/api.shtml to register with the RIM signing authority system for access to the controlled APIs and use the BlackBerry Signature Tool, which is a component of the BlackBerry JDE, to request, receive, and verify a digital code signature from RIM for the application.

Third party application developers who create controlled access third-party APIs can act as a signing authority for those APIs. The application developer can download and install the BlackBerry® Signing Authority Tool to allow other developers to register for access to the application developer's controlled APIs. Registered developers can use their BlackBerry Signature Tool to request, receive, and verify digital code signatures from the application developer's BlackBerry Signing Authority Tool for their applications.

Each third-party application requires authorization to run on the BlackBerry device. MIDlets (applications that use standard MIDP and CLDC APIs only) cannot write to memory on a BlackBerry device, access the memory of other applications, or access the persistent data of other MIDlets unless they are digitally signed by RIM's signing authority system. For more information about code signing and third-party applications, see the *BlackBerry Signing Authority Tool Administrator Guide*.

Using code signing on BlackBerry MDS Runtime Applications

Your organization's developers can digitally sign BlackBerry MDS Runtime Applications that they create using BlackBerry MDS Studio, before publishing these applications to the BlackBerry MDS Application Repository. BlackBerry devices support using a private key with a corresponding certificate in X.509 syntax to digitally sign BlackBerry MDS Runtime Applications.

BlackBerry MDS Runtime Applications communicate with enterprise systems through the BlackBerry MDS Integration Service, a component of the BlackBerry Enterprise Server. The BlackBerry MDS Integration Service verifies the digital signature on the BlackBerry MDS Runtime Application code before sending the application to BlackBerry devices over the wireless network. When the BlackBerry device receives the BlackBerry MDS Runtime Application, it displays the certificate subject details as the code signer identity, and prompts the BlackBerry device user to accept or reject the application.

The BlackBerry device does not display the code signer identity to the user, and does not install the application if any of the following conditions are true:

- the application is signed with an untrusted certificate
- the signature is invalid
- the Allow Unsigned Applications option is set to False for the BlackBerry MDS Integration Service, and the application is not digitally signed

Protecting lost, stolen, or replaced BlackBerry devices

The BlackBerry Enterprise Server administrator controls BlackBerry devices remotely to immediately protect confidential enterprise information using IT administration commands.

IT administration command	Description
Set Password and Lock Handheld	Use this command to create a new password and lock a lost BlackBerry device remotely. The BlackBerry Enterprise Server administrator can then verbally communicate the new password to the user when the user locates the BlackBerry device. When the user unlocks the BlackBerry device, the BlackBerry device prompts the user to accept or reject the new password change.
Erase Data and Disable Handheld	Use this command to remotely delete all user information and application data that the BlackBerry device stores. If a BlackBerry device is lost and might be recovered by the user, the BlackBerry Enterprise Server administrator can configure a delay, in hours, before the BlackBerry device starts the process of deleting all of its user information and application data. The BlackBerry Enterprise Server administrator can also specify whether to allow the user to terminate the process of erasing data from and making the BlackBerry device unavailable during the delay period. The BlackBerry Enterprise Server administrator can use this command to prepare a BlackBerry device for transfer between users in your organization.

For more information, see the *BlackBerry Enterprise Server System Administration Guide*.

Remotely resetting the password of a content protected BlackBerry device

The remote password reset cryptographic protocol is designed to allow the BlackBerry Enterprise Server administrator to set the BlackBerry device password remotely, even if content protection is enabled on the BlackBerry device. The BlackBerry device does not prompt the user for the old BlackBerry device password.

The cryptographic protocol for resetting the password on a content-protected device remotely is designed to provide the following features:

- allows the BlackBerry device to re-encrypt the content protection key with the new password, without knowing the old password
- prevents a hardware-based attack on the BlackBerry device from recovering the content protection key successfully without knowing either the BlackBerry device password or the IT policy private key of the IT policy public and private key pair that the BlackBerry Enterprise Server generates for the BlackBerry device
- prevents a small subgroup containment attack through the use of elliptic curve cryptography
- prevents the BlackBerry Enterprise Server from learning anything that an attacker could use to recover the content protection key

The BlackBerry Enterprise Server administrator should send the Set a Password and Lock Handheld IT administration command to a content-protected BlackBerry device that is in the possession of the BlackBerry device user only. Sending this command to a BlackBerry device in the possession of an attacker allows an attacker that uses a hardware-based attack to recover the key pair that the BlackBerry device creates when it receives the IT policy from flash memory, and thereby decrypt all the data on the BlackBerry device.

For more information about the protocol, see "Appendix L: Protocol for resetting the password on a content-protected BlackBerry device remotely" on page 88.

Remotely erasing data from BlackBerry device memory and making the BlackBerry device unavailable

A BlackBerry device that is not physically connected to a computer is designed to permanently delete its user and application data when any of the following events occur:

- The user clicks Wipe Device (in the Security Options) on the BlackBerry device.
- The user types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule allows on the BlackBerry device. (The default is ten attempts.)
- The BlackBerry Enterprise Server administrator sends the Erase Data and Disable Handheld IT administration command to the BlackBerry device from the BlackBerry Manager.
- The BlackBerry Enterprise Server administrator sends the Erase Data and Disable Handheld IT administration command with a delay (in hours, up to 168 hours) to the BlackBerry device from the BlackBerry Manager.

The BlackBerry Enterprise Server administrator can also set the following IT policy rules to require that the remote BlackBerry device automatically delete its user and application data.

IT policy rule	Description
Secure Wipe Delay After IT Policy Received	Set this IT policy rule to a period of time, in hours, after which, if the BlackBerry device has not successfully received IT policy updates or IT administration commands, the BlackBerry device permanently deletes its user and application data.
Secure Wipe Delay After Lock	Set this IT policy rule to a period of time, in hours, after which, if the user has not unlocked the BlackBerry device, the BlackBerry device permanently deletes its user and application data.

IT policy rule	Description
Secure Wipe if Low Battery	Set this IT policy rule to require that, if the BlackBerry device battery power is insufficient to receive IT policy updates or IT administration commands, the BlackBerry device permanently deletes its user and application data.

The BlackBerry device wipe process is designed to delete all data in memory and overwrite memory with zeroes. If content protection is turned on, the BlackBerry device also uses a memory scrub process to overwrite the BlackBerry device flash memory file system. The BlackBerry memory scrub process complies with United States government requirements for clearing sensitive user data, including Department of Defense directive 5220.22-M and National Institute of Standards and Technology Special Publication 800-88.

When the BlackBerry device permanently deletes its stored user and application data, it also performs the following actions:

BlackBerry device action	Description
delete the master encryption key	The BlackBerry device deletes its references to the master encryption key in memory.
unbind the IT policy	The BlackBerry device deletes the IT policy public key from its NV store so that it can receive a new IT policy and digitally signed IT policy public key from a BlackBerry Enterprise Server. The BlackBerry device does not delete its stored IT policy.
unbind the smart card (if applicable)	The BlackBerry device deletes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.

For more information, see "Appendix D: BlackBerry device wipe process" on page 74.

Remotely resetting a BlackBerry device to factory default settings

The BlackBerry Enterprise Server administrator can use the Remote Wipe Reset to Factory Defaults IT policy rule to require the BlackBerry device to return to factory default settings when it receives the Erase Data and Disable Handheld IT administration command over the wireless network. When the BlackBerry Enterprise Server administrator sets this rule to True and sends the Erase Data and Disable Handheld IT administration command to the BlackBerry device from the BlackBerry Manager, the BlackBerry device performs the following actions:

- permanently deletes its stored IT policy
- permanently deletes all third-party applications
- permanently deletes all user data

Erasing all data and applications from the BlackBerry device memory over a physical connection

A BlackBerry device is designed to erase its user and application data and all applications when it is physically connected to a computer and any of the following events occur:

- The BlackBerry device user runs the application loader tool in the BlackBerry Desktop Software and types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule allows in the application loader tool prompt. (The default is ten attempts.)

  The BlackBerry device user can also use the application loader tool in the BlackBerry Desktop Software to erase all user and application data on the BlackBerry device, but choose not to erase the BlackBerry device applications.
- The BlackBerry Enterprise Server administrator clicks Wipe Handheld File System in the BlackBerry Manager. This option deletes all data and applications from the BlackBerry device even if the service books

do not exist on the BlackBerry device (in other words, if there is no connection between the BlackBerry Enterprise Server and the BlackBerry device).

- The BlackBerry Enterprise Server administrator clicks Nuke Handheld in the BlackBerry Manager. This option overwrites all contents in BlackBerry device memory with zeroes.

Unbinding the smart card from the BlackBerry device

When the BlackBerry Enterprise Server administrator or the user starts a BlackBerry device wipe, causing the BlackBerry device to erase its stored user and application data, the BlackBerry device permanently deletes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.

The BlackBerry Enterprise Server administrator can permanently delete the smart card binding information from the BlackBerry device manually in the following ways.

- Send the Erase Data and Disable Handheld IT administration command to the BlackBerry device to permanently delete the binding between a user's current smart card and the BlackBerry device.
- When the user turns off two-factor authentication, the BlackBerry device turns off two-factor authentication with the installed smart card and permanently deletes the smart card binding information from the BlackBerry device.

Related resources

Resource	Information
BlackBerry Enterprise Server Feature and Technical Overview	• BlackBerry Enterprise Server architecture
BlackBerry Enterprise Server Wi-Fi Implementation Supplement	• understanding configuration options for implementing a BlackBerry device on an enterprise Wi-Fi network • administering and troubleshooting a BlackBerry device on an enterprise Wi-Fi network
BlackBerry Enterprise Server Installation Guide	• network environment settings • messaging and collaboration environment settings • database environment settings
BlackBerry Enterprise Server System Administration Guide	• generating and changing master encryption keys • enabling encryption • managing security
BlackBerry Enterprise Solution Security Acronym Glossary	• full terms substituted by acronyms in this and other security documents
BlackBerry Signing Authority Tool Administrator Guide	• the BlackBerry Signing Authority Tool implementation of public key cryptography • installing, setting up, and managing the BlackBerry Signing Authority Tool • restricting access to APIs
BlackBerry Java Development Environment BlackBerry Application Developer Guide Volume 1	• using BlackBerry APIs • APIs, classes, and methods with limited access • retrieving custom IT policy rules from the IT policy API • deploying applications using the BlackBerry Desktop Software • deploying applications over the wireless network
BlackBerry Java Development Environment BlackBerry Application Developer Guide Volume 2	• using controlled APIs • code signatures
BlackBerry Smart Card Reader Security Technical Overview	• secure pairing between the BlackBerry device and the BlackBerry Smart Card Reader • initial key establishment protocol • connection key establishment protocol
BlackBerry Wireless Enterprise Activation Technical Overview	• wireless enterprise activation process • wireless master encryption key generation • initial key establishment protocol • key rollover protocol

Resource	Information
Garbage Collection in the BlackBerry Java Development Environment	• cleaning BlackBerry device memory
Policy Reference Guide	• list of BlackBerry Enterprise Server IT policy rules, application control policy rules, and MDS policy rules • using IT policies, application control policies, and MDS policies
PGP Support Package for BlackBerry devices Security Technical Overview	• PGP security and encryption • using PGP Universal Server to store and manage PGP keys • searching for and validating PGP keys • sending and receiving PGP messages
PGP Support Package User Guide Supplement	• installing the PGP Support Package for BlackBerry devices • managing PGP keys on the BlackBerry device • setting PGP options for digitally signing and encrypting messages
Placing the BlackBerry Enterprise Solution in a Segmented Network	• using segmented network architecture to prevent the spread of malware on your organization's network
Protecting the BlackBerry device platform against malware	• understanding the BlackBerry device application platform default behavior • understanding malware vulnerabilities on the BlackBerry device • managing the risk of malware attacks • using BlackBerry Enterprise Solution tools to contain malware on the BlackBerry device
S/MIME Support Package for BlackBerry devices Technical Overview	• S/MIME security and encryption • managing S/MIME certificates on the BlackBerry device and computer
S/MIME Support Package User Guide Supplement	• installing the S/MIME Support Package for BlackBerry devices • managing certificates on the BlackBerry device and computer • setting S/MIME options for digitally signing and encrypting messages • sending and receiving S/MIME messages
Security for BlackBerry Devices with Bluetooth Wireless Technology	• Bluetooth wireless technology overview • using and protecting Bluetooth enabled BlackBerry devices • risks of using Bluetooth wireless technology on mobile devices

Resource	Information
Visit www.blackberry.com/security.	• information about BlackBerry Solution security

Appendix A: RIM Crypto API Interface

The RIM Crypto API on the BlackBerry device and in the BlackBerry JDE provides developers with a toolkit of cryptographic algorithms and support tools that they can use to create secure applications for business connectivity. RIM uses code signing to authorize running secure applications on the BlackBerry device and to control third-party application access to the RIM Crypto API.

The RIM Crypto API consists of a Java interface and algorithms for the following components:

- schemes for encryption, key agreements, and signatures
- a key generation protocol
- code for message authentication, message digests, and hashes

Developers can use the JDE Java interface to access the RIM Crypto API encryption algorithms and other code to create simple solutions. Developers do not need to modify or directly access the encryption code because all calls to the native C++ encryption code are routed through the JDE Java code.

Cryptographic functionality that the RIM Crypto API provides

Symmetric block algorithms

Algorithm (uses PKCS #5 for padding)	Key length (bits)	Modes (implemented separately from the block encryption algorithms)
AES	128, 192, and 256	ECB, CBC, CFB, OFB, X
DES	56	ECB, CBC, CFB, OFB, X
RC2	8 to 1024	ECB, CBC, CFB, OFB, X
RC5	0 to 2040	ECB, CBC, CFB, OFB, X
Skipjack	80	ECB, CBC, CFB, OFB, X
Triple DES	112 and 168	ECB, CBC, CFB, OFB, X
CAST5-128	128	ECB, CBC, CFB, OFB, X

Symmetric stream encryption algorithms

Algorithm	Key length (bits)
ARC4	unlimited

Asymmetric stream encryption algorithms

Algorithm	Key length (bits)
ECIES	unlimited (160 to 571 for seeding)

Asymmetric encryption algorithms

Algorithm	Key length (bits)	Type
RSA raw	512 to 4096	integer factorization
RSA with PKCS #1 formatting (version 1.5 and 2.0)	512 to 4096	integer factorization
RSA with OAEP formatting	512 to 4096	integer factorization
El Gamal	512 to 4096	discrete logarithm

Key agreement scheme algorithms

Algorithm	Key length (bits)	Type
DH	512 to 4096	discrete logarithm
KEA	1024	discrete logarithm
ECDH	160 to 571	(EC) discrete logarithm
ECMQV	160 to 571	(EC) discrete logarithm

Signature scheme algorithms

Algorithm	Key length (bits)	Type
DSA	512 to 1024	discrete logarithm
RSA using PKCS #1 (version 1.5 and 2.0)	512 to 4096	integer factorization
RSA using ANSI X9.31 **Note**: ANSI X9.31 uses one of the following algorithms for the required message digest code: SHA-1, SHA-256, SHA-384 or SHA-512, or RIPEMD-160.	512 to 4096	integer factorization
RSA using PSS	512 to 4096	integer factorization
ECDSA	160 to 571	(EC) discrete logarithm
ECNR	160 to 571	(EC) discrete logarithm

Key generation algorithms

Algorithm	Key length (bits)	Type
RSA	512 to 2048	integer factorization
DH	512 to 4096	discrete logarithm
DSA	512 to 1024	discrete logarithm
EC	160 to 571	(EC) discrete logarithm

Message authentication codes

Code	Key length (bits)
CBC MAC	variable (block cipher key length)
HMAC	variable

Message digest codes

Code	Digest length (bits)
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	160, 224, 256, 384, 512
MD2	128
MD4	128
MD5	128

Code	Digest length (bits)
RIPEMD-128, 160	128, 160

Appendix B: TLS and WTLS standards that the RIM Crypto API supports

The TLS and WTLS protocol cipher suite components that the RIM Crypto API supports apply only to WTLS and handheld (direct) mode TLS/SSL on the BlackBerry device.

The RIM Crypto API implementation of the TLS and WTLS protocols supports the use of RSA and DSA public key algorithms and the DH key exchange algorithm, with the following limitations:

Cipher suite type	Typical component limitation (in bits)
export	• RSA and DH: 1024 bits or less • EC: 163 bits or less
non export	• non elliptic curve operations: 4096 bits • elliptic curve operations: 571 bits **Note**: These limitations are due to computational constraints on the BlackBerry device.

Key establishment algorithm cipher suites that the RIM Crypto API supports

Direct mode SSL	Direct mode TLS	WTLS
RSA_EXPORT	RSA_EXPORT	RSA_anon
DH_anon_EXPORT	DH_anon_EXPORT	RSA_anon_512
DHE_DSS_EXPORT	DHE_DSS_EXPORT	RSA_anon_768
RSA	RSA	RSA
DHE_DSS	DHE_DSS	RSA_512
DH_anon	DH_anon	RSA_768
		DH_anon
		DH_anon_512
		DH_anon_768

Symmetric algorithms that the RIM Crypto API supports

Direct mode SSL	Direct mode TLS	WTLS
RC4 40	RC4 40	RC5 40
DES 40	RC4 56	RC5 56
DES	RC4 128	RC5 64
Triple DES	DES 40	RC5
RC4 128	DES	RC5 128
	Triple DES	DES 40
	AES 128	DES
	AES 256	Triple DES
	RC4 128	

Hash algorithms that the RIM Crypto API supports

Direct mode SSL	Direct mode TLS	WTLS
MD5	MD5	SHA
SHA-1	SHA-1	SHA-40
		SHA-80
		MD5
		MD5 40
		MD5 80

© 2008 Research In Motion Limited. All rights reserved.

Appendix C: Previous version of wired master encryption key generation

Each time a BlackBerry Enterprise Server or BlackBerry Desktop Software version earlier than 4.0 calls the master encryption key generation function, the C language srand function is seeded with the current time to generate a seed for the C language rand function. When the user responds to the BlackBerry Desktop Software prompt by moving the mouse, the rand function is designed to generate random data based on the entropy that the mouse movement gathers.

Previous version of wired master encryption key generation process

1. When the user moves the mouse, the BlackBerry Enterprise Server or BlackBerry Desktop Software generates either 2 or 4 bits, depending on whether one or both of the x and y axes have changed. The BlackBerry Enterprise Server or BlackBerry Desktop Software samples bits in this way until accumulating at least 8 bits.
2. The rand function generates a random integer.
3. The BlackBerry Enterprise Server or BlackBerry Desktop Software examines the integer's least significant bit. If the bit is a 1, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores 1's complement of the 8 accumulated bits; otherwise, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores the 8 accumulated bits unmodified. This process is designed to make sure that, even if a user replicates a previous user's mouse movements (which is virtually impossible), the resulting value is still unique.
4. The algorithm loops until the BlackBerry Enterprise Server or BlackBerry Desktop Software has sampled 256 random bits from the user's mouse movements.
5. The BlackBerry Enterprise Server or BlackBerry Desktop Software uses the SHA-1 function to hash the 256 bits.
6. The BlackBerry Enterprise Server or BlackBerry Desktop Software generates the master encryption key using the first 128 bits of the resulting hash.

© 2008 Research In Motion Limited. All rights reserved.

Appendix D: BlackBerry device wipe process

A BlackBerry device wipe is designed to delete and overwrite the BlackBerry device memory using the following process:

1. The BlackBerry device sets a Device Under Attack flag in the NV store.

   If a user removes the battery before the BlackBerry device data wipe ends, when the BlackBerry device power is restored (in other words, a user replaces the battery), the BlackBerry device wipe process continues because the Device Under Attack flag is still present.
2. If content protection of master encryption keys is turned on, the BlackBerry device overwrites the copy of the grand master key in RAM with zeroes.
3. The BlackBerry device deletes its binding with the BlackBerry Enterprise Server by deleting the IT policy public key from the NV store.
4. If applicable, the BlackBerry device deletes the smart card binding information from the NV store.
5. The BlackBerry device wireless transceiver turns off.
6. The BlackBerry device deletes data in the persistent store in flash memory, including references to the master encryption key.
7. The BlackBerry device overwrites flash memory with zeroes.
8. The BlackBerry device memory scrub process overwrites the BlackBerry device heap in RAM, changing the state of each bit four times. For more information, see "Memory scrub process for RAM" below.
9. The BlackBerry device clears the BlackBerry device password from the NV store.
10. If content protection is turned on, the BlackBerry device memory scrub process overwrites the BlackBerry device flash memory file system, changing the state of each bit four times. For more information, see "Memory scrub process for flash memory" below.
11. The BlackBerry device clears the Device Under Attack flag from the NV store.
12. The BlackBerry device restarts.

Memory scrub process for RAM

The BlackBerry device memory scrub process performs the following actions to overwrite the BlackBerry device heap in RAM:

1. Writes 0x33 to each byte ($0011\ 0011_2$).
2. Clears all bytes to 0x00 ($0000\ 0000_2$).
3. Writes 0xCC to each byte ($1100\ 1100_2$).
4. Clears all bytes to 0x00 ($0000\ 0000_2$).
5. Writes 0x55 to each byte ($0101\ 0101_2$).
6. Clears all bytes to 0x00 ($0000\ 0000_2$).
7. Writes 0xAA to each byte ($1010\ 1010_2$).

Memory scrub process for flash memory

If content protection is enabled, the BlackBerry device memory scrub process performs the following actions to overwrite the BlackBerry device flash memory during a BlackBerry device wipe:

1. Writes 0x33 to each byte ($0011\ 0011_2$).
2. Clears all bytes to 0xFF to each byte ($1111\ 1111_2$).
3. Writes 0xCC to each byte ($0x1100\ 1100_2$).

© 2008 Research In Motion Limited. All rights reserved.

4. Clears all bytes to 0xFF ($1111\ 1111_2$).
5. Writes 0x55 to each byte ($0x0101\ 0101_2$).
6. Clears all bytes to 0xFF ($1111\ 1111_2$).
7. Writes 0xAA to each byte ($0x1010\ 1010_2$).
8. Clears all bytes to 0xFF ($1111\ 1111_2$).

© 2008 Research In Motion Limited. All rights reserved.

Appendix E: Ephemeral AES encryption key derivation process

The BlackBerry device uses an ephemeral 256-bit AES encryption key to encrypt the content protection key and the ECC private key. The BlackBerry device derives the ephemeral 256-bit AES encryption key from the BlackBerry device password using the following process:

1. The BlackBerry device selects a 64-bit salt (random data to mix with the BlackBerry device password). This is intended to keep two identical passwords from turning into the same key.
2. The BlackBerry device concatenates the salt, the password, and the salt again into a byte array (Salt|Password|Salt).
3. The BlackBerry device hashes the byte array with SHA-256.
4. The BlackBerry device stores the resulting hash in a byte array called a key.

   (key) = SHA256(Salt|Password|Salt)
5. The BlackBerry device hashes (key) 18 more times. It stores the result into (key) each time. For example, for i=0 to 18, the BlackBerry device does the following:

   (key) = SHA256(key)

   i++

   done
6. The final hash creates the ephemeral key.

For more information, see the *RSA Security – PKCS #5*.

© 2008 Research In Motion Limited. All rights reserved.

Appendix F: Power and electromagnetic side-channel attacks and countermeasures

The BlackBerry device implementation of AES is designed to protect user data and encryption keys from traditional and side-channel attacks.

Attack type	Description
traditional	• attacks data that the cryptographic system stores or transmits • attempts to determine the user's encryption key or the plain text data by exploiting a weakness in the design of the cryptographic algorithm or protocol
side-channel	• attempts to exploit physical properties of the algorithm implementation using power analysis (for example, SPA and DPA) and electromagnetic analysis (for example, SEMA and DEMA) • attempts to determine the encryption keys that a device uses by measuring and analyzing the power consumption, or electromagnetic radiation that the device emits during cryptographic operations

The BlackBerry device uses a masking operation, table splitting, and application of random masks to help protect the cryptographic keys and plain text data against side-channel attacks at all points during its encryption and decryption operations.

Masking operation process that the AES implementation uses when content protection is turned on

During the initial AES algorithm calculation, the following actions occur:

1. The BlackBerry device performs the masking operation by
   - creating a mask table (M), where each table entry is a random value
   - creating a masked version of the S-Box table (S') used within AES
   - periodically and randomly permuting all table entries
2. The BlackBerry device runs the input through both M and S'.
3. The BlackBerry device combines the output from M and S'.
4. The BlackBerry device removes the mask and produces the AES output.

During subsequent AES algorithm calculations, the following actions occur:

1. The BlackBerry device performs the masking operation by periodically and randomly permuting all table entries in every calculation.
2. The BlackBerry device runs the input through both M and S'.
3. The BlackBerry device combines the output from M and S'.
4. The BlackBerry device removes the mask and produces the AES output.

Masking operation process that the AES implementation uses when content protection is turned off

The AES algorithm calculation that BlackBerry devices use when content protection is turned off consists of the following stages:

1. The BlackBerry device masks the output from the round key.
2. The BlackBerry device masks the AES S-Box input.
3. The BlackBerry device masks the AES S-Box output.

© 2008 Research In Motion Limited. All rights reserved.

How the AES algorithm creates S-Box tables

The BlackBerry device permutes each AES S-Box entry randomly and masks each entry with a random value.

How the AES algorithm calculation uses round keys

The BlackBerry device masks the round keys (subkeys that the key schedule calculates for each round of encryption) with random values and any S-Box masks that the AES algorithm requires to operate.

How the AES algorithm calculation uses masks

The BlackBerry device changes the random masks periodically and uses extra S-Box data to make identification of the S-Box table difficult, whether the S-Box table is used in the encryption, decryption, or key schedule process.

© 2008 Research In Motion Limited. All rights reserved.

Appendix G: BlackBerry Router protocol

When the BlackBerry Enterprise Server and the BlackBerry device use the BlackBerry Router protocol to open a connection between them, the BlackBerry Router protocol is designed to use its unique authentication protocol to verify that the BlackBerry device has the correct master encryption key while preventing the BlackBerry Router from knowing the value of the master encryption key. To accomplish this, the BlackBerry Router protocol uses two runs of the elliptic curve version of the Schnorr identification scheme to provide mutual authentication between the BlackBerry device and the BlackBerry Enterprise Server.

The BlackBerry Enterprise Server and the BlackBerry Router also use the BlackBerry Router protocol to close an authenticated connection to the BlackBerry device. The BlackBerry Router protocol is designed to allow only an authenticated party to close the connection by using one run of the Schnorr identification scheme to authenticate the close command that the BlackBerry Enterprise Server sends to the BlackBerry Router.

The BlackBerry Router, the BlackBerry Enterprise Server, and the BlackBerry device are designed to share the following cryptosystem parameters when using the BlackBerry Router protocol.

Parameter	Description
E(Fq)	the NIST-approved 521-bit random elliptic curve over *Fq*, which has a cofactor of 1; the BlackBerry Router authentication protocol does all math operations in the group *E(Fq)* and Z_p
Fq	a finite field of prime order *q*
P	a point of *E* that generates a prime subgroup of *E(Fq)* of order *p*
xR	a representation of elliptic curve scalar multiplication, where *x* is the scalar and *R* is a point on *E(Fq)*
s	the master encryption key value
h	the SHA-512 hash of *s*

How the BlackBerry Router protocol uses the Schnorr identification scheme

The implementation of the Schnorr identification scheme in the BlackBerry Router protocol uses a group of large prime order, the additive group of elliptic curve points for a prime p.

The BlackBerry Router protocol is designed to use the following security measures:

- uses the NIST recommended 521 bit elliptic curve group
- verifies that points supplied by the parties involved in the communication are members of the Elliptic Curve group
- verifies that R_D does not equal R_B, to prevent recovery of *h* by an attacker
- verifies that *e* does not equal 0, to prevent recovery of *h* by an attacker
- verifies that R does not equal the point at infinity, to verify that R is a valid public key
- verifies that *R* does not equal the point at infinity, to verify that *R* is a valid public key
- resets any malformed data that it finds to a random value so that the protocol can proceed past the point at which it detects malformed data, allowing the protocol to fail at completion only; this measure is designed to prevent various types of timing attacks

Examples of attacks that the BlackBerry Router protocol is designed to prevent

Impersonating a BlackBerry device

An impersonation of the BlackBerry device occurs when the attacker sends messages to the BlackBerry Enterprise Server so that the BlackBerry Enterprise Server believes it is communicating with the BlackBerry

© 2008 Research In Motion Limited. All rights reserved.

device. The attacker must send master encryption key value (*s*) to the BlackBerry Enterprise Server, which requires effectively solving the discrete log problem to determine *s* or the hash of *s*.

Impersonating a BlackBerry Enterprise Server

An impersonation of the BlackBerry Enterprise Server occurs when the attacker sends messages to the BlackBerry device so that the BlackBerry device believes it is communicating with the BlackBerry Enterprise Server. The attacker must send *s* to the BlackBerry device, which requires effectively solving the discrete log problem to determine *s* or the hash of *s*.

Process flow: Using the BlackBerry Router protocol to open an authenticated connection

1. The BlackBerry device and the BlackBerry Enterprise Server both hash the current BlackBerry device master encryption key using SHA-512.
2. The BlackBerry device picks a random value r_D, where $1 < r_D < p - 1$ and calculates $R_D = r_D P$.
3. The BlackBerry device sends R_D and *KeyID*, a master encryption key identifier, to the BlackBerry Enterprise Server.
4. The BlackBerry Router observes the data that the BlackBerry device sends and confirms that the value R_D is not the point at infinity. If R_D is the point at infinity, the BlackBerry Router sets R_D to a random value.
5. The BlackBerry Router forwards R_D and *KeyID* to the BlackBerry Enterprise Server.
6. The BlackBerry Enterprise Server calculates that as R_D approaches the point at infinity, R_D is random.
7. The BlackBerry Enterprise Server picks a random value r_B, where $1 < r_B < p - 1$ and calculates $R_B = r_B P$.

   If R_D equals R_B, the BlackBerry Enterprise Server calculates another value of R_B.
8. The BlackBerry Enterprise Server picks a random value e_D, where $1 < e_D < p - 1$.
9. The BlackBerry Enterprise Server sends R_B, e_D, and *KeyID* to the BlackBerry device.
10. The BlackBerry Router observes the data that the BlackBerry Enterprise Server sends and confirms the following calculations:
    - checks that when the value R_B approaches the point at infinity or R_D equals R_B, the value R_B is random
    - checks that when the value e_D equals 0, the value e_D is random
11. The BlackBerry Router forwards R_B, e_D, and *KeyID* to the BlackBerry device.
12. The BlackBerry device performs the following calculations:
    - checks that when the value R_B approaches the point at infinity or R_D equals R_B, the value R_B is random
    - checks that when the value e_D equals 0, the value e_D is random
    - computes $y_D = h - e_D r_D \bmod p$
13. The BlackBerry device picks a random value e_B, where $1 < e_B < p - 1$.
14. The BlackBerry device sends y_D and e_B to the BlackBerry Enterprise Server.
15. The BlackBerry Router observes the data that the BlackBerry device sends and confirms that if e_B equals 0 or e_B equals e_D, the value e_B is random.
16. The BlackBerry Router forwards y_D and e_B to the BlackBerry Enterprise Server.
17. The BlackBerry Enterprise Server performs the following calculations:
    - checks that when the value e_D equals e_B, the value e_B is random
    - checks that when the value e_D equals 0, the value e_D is random
    - computes $y_B = h - e_B r_B \pmod p$
18. The BlackBerry Enterprise Server sends y_B to the BlackBerry device.
19. The BlackBerry device receives y_B.

© 2008 Research In Motion Limited. All rights reserved.

If the BlackBerry device accepts y_B, the BlackBerry Enterprise Server and the BlackBerry device open an authenticated connection between them.

If the BlackBerry device calculates that $y_BP + e_BR_B \neq hP$, the BlackBerry device rejects the connection attempt. The BlackBerry Enterprise Server and the BlackBerry device do not open an authenticated connection between them.

If the BlackBerry Router calculates that $y_BP + e_BR_B \neq y_DP + e_DR_D$, the BlackBerry Router rejects the connection attempt.

If the BlackBerry Enterprise Server calculates that $y_DP + e_DR_D \neq hP$, the BlackBerry Enterprise Server rejects the connection attempt.

20. The BlackBerry Router stores R_D, R_B, $y_DP + e_DR_D$, e_D, and e_B.
21. The BlackBerry Enterprise Server stores R_D, R_B, e_D, e_B, and h.
22. The BlackBerry Router and the BlackBerry Enterprise Server overwrite y_B and y_D in memory with zeroes.

Process flow: Using the BlackBerry Router protocol to close an authenticated connection

1. The BlackBerry Enterprise Server picks a random value r_C, where $1 < r_c < p - 1$.
2. The BlackBerry Enterprise Server calculates $R_C = r_CP$.

   If R_C equals R_B, or R_B equals R_D the BlackBerry Enterprise Server calculates another R_C value.
3. The BlackBerry Enterprise Server sends the value R_C to the BlackBerry Router to initiate connection closure.
4. The BlackBerry Router performs the following calculations:
   - checks that when the value R_C approaches the point at infinity, the value R_C is random
   - checks that when the value R_C equals R_B, or R_B equals R_D, the value R_C is random
5. The BlackBerry Router picks a random value e_C, where $1 < e_c < p - 1$.

   If e_C equals e_D, or e_c equals e_B the BlackBerry Router calculates another e_C value.
6. The BlackBerry Router sends the value e_C to the BlackBerry Enterprise Server.
7. The BlackBerry Enterprise Server performs the following calculations:
   - checks that when the value e_C equals 0, the value e_C is random
   - checks that when the value e_C equals e_B, or e_C equals e_D, the value e_C is random
8. The BlackBerry Enterprise Server calculates $y_C = h - e_Cr_C \bmod p$.
9. The BlackBerry Enterprise Server sends the value y_C to the BlackBerry Router.

   If the BlackBerry Router accepts y_C, the BlackBerry Router closes the authenticated connection to the BlackBerry device on behalf of the BlackBerry Enterprise Server.

   If the BlackBerry Router calculates that $y_CP + e_CR_C \neq y_DP + e_DR_D$, the BlackBerry Router rejects the connection close attempt. The BlackBerry Router does not close the authenticated connection to the BlackBerry device.

© 2008 Research In Motion Limited. All rights reserved.

Appendix H: Enterprise Wi-Fi security methods that the BlackBerry device supports

EAP authentication methods that the BlackBerry device supports

The BlackBerry device supports EAP authentication methods with protected WLAN networks only.

Authentication method	Description	BlackBerry device implementation
LEAP	Cisco® developed LEAP in response to the weaknesses identified in WEP. LEAP uses the IEEE 802.1x authentication framework. LEAP is designed to significantly improve on basic WEP security by providing authentication between the enterprise Wi-Fi network device and the enterprise Wi-Fi network, per-client dynamic generation of WEP keys, and automatic WEP key updates throughout the course of a session on the enterprise Wi-Fi network device.	The BlackBerry device supports LEAP authentication based on a user name and password. The BlackBerry device uses a one-way function to encrypt passwords before sending them to the authentication server. LEAP does not provide mutual authentication between the BlackBerry device and the enterprise Wi-Fi network. Set strong password policies on networks that use LEAP.
PEAP	PEAP is an open standard jointly developed by Microsoft Corporation, RSA Security, and Cisco Systems, Inc. PEAP allows for supplicant authentication with an authentication server by • creating an encrypted tunnel between the supplicant and the authentication server using TLS • using the TLS tunnel to send the supplicant authentication credentials to the authentication server	The BlackBerry device supports the following versions of PEAP: • PEAPv0 • PEAPv1 The BlackBerry device supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols that the BlackBerry device can use with PEAP for the authentication credential exchange. A root certificate corresponding to the server certificate that the authentication server uses must exist on the BlackBerry device for PEAP authentication to complete successfully.
EAP-TLS	EAP-TLS is defined in RFC 2716. It uses a PKI to enable supplicant authentication with an authentication server by • using the TLS protocol to create an encrypted tunnel between the supplicant and the authentication server • using the TLS encrypted tunnel and a client certificate to send authentication credentials to the authentication server	The Wi-Fi enabled BlackBerry device supports EAP-TLS using certificates that meet specific requirements on both the server and the client for successful authentication. The root certificates of the authentication server certificate and the client certificate must exist on the Wi-Fi enabled BlackBerry device for EAP-TLS authentication to complete successfully.

© 2008 Research In Motion Limited. All rights reserved.

Authentication method	Description	BlackBerry device implementation
EAP-TTLS	EAP-TTLS is designed to extend EAP-TLS by enabling authentication from the authentication server to the supplicant. When the authentication server has used its certificate to authenticate to the supplicant successfully and established a secure connection to the BlackBerry device, the server can use an authentication protocol over the established secure connection to authenticate the supplicant.	The BlackBerry device supports EAP-MS-CHAPv2 and MS-CHAPv2 as second-phase protocols that the BlackBerry device can use with EAP-TTLS for the authentication credential exchange. The root certificates of the authentication server certificate need to exist on the Wi-Fi enabled BlackBerry device for EAP-TTLS authentication to complete successfully.
EAP-FAST	EAP-FAST is defined in RFC 4851. EAP-FAST uses PAC dynamically to establish a TLS connection to the BlackBerry device and verify the supplicant credentials over the TLS connection.	The BlackBerry device supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols that the BlackBerry device can use with EAP-FAST for the authentication credential exchange.
EAP-SIM	EAP-SIM is defined in RFC 4186. It uses the GSM SIM for authentication and session key distribution. GSM SIM authentication uses a challenge-response method without mutual authentication.	The BlackBerry device supports using EAP-SIM with the credentials on the GSM SIM only. The user does not need to type or select credentials on the BlackBerry device. The user identity that EAP-SIM uses for authentication on the BlackBerry device is built from the IMSI according to the 3GPP technical specification 3GPP-TS-23.003. The BlackBerry device can receive at least two challenges from the authentication server to provide stronger authentication.

Encryption algorithms that the BlackBerry device supports for use with layer 2 security methods

Protocol	Description	Wi-Fi enabled BlackBerry device implementation
WEP	For more information about WEP, see "Requiring protected connections to enterprise Wi-Fi networks" on page 50.	The Wi-Fi enabled BlackBerry device supports the use of WEP keys.

© 2008 Research In Motion Limited. All rights reserved.

Protocol	Description	Wi-Fi enabled BlackBerry device implementation
TKIP	TKIP is • part of the IEEE 802.11i enterprise Wi-Fi network security standard • designed to address the shortcomings in WEP without requiring replacement of the existing enterprise Wi-Fi network hardware • designed to use the RC4 encryption method (based on improved WEP standards) TKIP is designed to be more robust than WEP in the following ways: • using a key size of 128 bits (compared to 40 bits or 104 bits for WEP) • using a modified initialization vector, that is designed to significantly increase the difficulty of deriving the WEP key • generating keys dynamically for each session by changing keys automatically for each packet of transmitted data (where WEP uses a single fixed key for an entire session) • using a MIC that fails and discards transmitted packets that are captured, altered, and resent • requiring a secure method of distribution to a wireless client	The Wi-Fi enabled BlackBerry device supports the use of TKIP with • EAP-TLS • EAP-TTLS • EAP-FAST • PEAP • PSK
AES-CCMP	AES-CCMP is • part of the IEEE 802.11i enterprise Wi-Fi network security standard • designed to use AES encryption AES-CCMP is designed to provide a robust security protocol similar to TKIP in the following ways: • using a key size of 128 bits • using a MIC that fails and discards transmitted packets that are captured, altered, and resent • requiring a secure method of distribution to a wireless client	The Wi-Fi enabled BlackBerry device supports the use of AES-CCMP with • EAP-TLS • EAP-TTLS • EAP-FAST • PEAP • PSK

EAP authentication methods and encryption algorithms with which the BlackBerry device supports the use of CCKM

The Wi-Fi enabled BlackBerry device supports the use of CCKM with

- all EAP authentication methods that the Wi-Fi enabled BlackBerry device supports
- WEP and TKIP

The Wi-Fi enabled BlackBerry device does not support the use of CCKM with

- the Cisco CKIP encryption algorithm
- the AES-CCMP encryption algorithm

© 2008 Research In Motion Limited. All rights reserved.

VPN solution on the Wi-Fi enabled BlackBerry device

The Wi-Fi enabled BlackBerry device has a built-in VPN client that supports several VPN concentrators. Visit www.blackberry.com/products/wlan/sys_req.shtml for a list of currently supported VPN concentrators.

If the Wi-Fi enabled BlackBerry device has a VPN profile, it logs into the VPN concentrator automatically after connecting to the enterprise Wi-Fi network. To create a VPN profile, the BlackBerry Enterprise Server administrator must configure the VPN client settings (for example, the IP address of the VPN concentrator, user names and passwords, and cryptographic methods to be used) on the Wi-Fi enabled BlackBerry device, or on the BlackBerry Enterprise Server using IT policy rules. Depending on the security policy of your organization, the BlackBerry Enterprise Server administrator or the BlackBerry device user can save each user name and password to the Wi-Fi enabled BlackBerry device to prevent the Wi-Fi enabled BlackBerry device from prompting the user for credentials the first time (or each time) that the Wi-Fi enabled BlackBerry device connects to the enterprise Wi-Fi network.

The Wi-Fi enabled BlackBerry device is also compatible with VPN environments that use two-factor authentication using hard tokens or software tokens for user credentials. When the Wi-Fi enabled BlackBerry device tries to log into the VPN, the Wi-Fi enabled BlackBerry device uses automatically generated or user-provided credentials with the hard token or software token.

Appendix I: Algorithm suites that the BlackBerry device supports for negotiating SSL connections

Wi-Fi enabled BlackBerry devices support the following direct mode TLS algorithm suites for negotiating SSL connections to the BlackBerry Infrastructure.

- DH_anon_WITH_3DES_EDE_CBC_SHA
- DH_anon_WITH_AES_128_CBC_SHA
- DH_anon_WITH_AES_256_CBC_SHA
- DH_anon_WITH_DES_CBC_SHA
- DH_anon_WITH_RC4_128_MD5
- DH_anon_EXPORT_WITH_DES40_CBC_SHA
- DH_anon_EXPORT_WITH_RC4_40_MD5
- DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- DHE_DSS_WITH_3DES_EDE_CBC_SHA
- DHE_DSS_WITH_AES_128_CBC_SHA
- DHE_DSS_WITH_AES_256_CBC_SHA
- DHE_DSS_WITH_DES_CBC_SHA
- DHE_RSA_WITH_AES_128_CBC_SHA
- DHE_RSA_WITH_AES_256_CBC_SHA
- DHE_RSA_WITH_3DES_EDE_CBC_SHA
- DHE_RSA_WITH_DES_CBC_SHA
- RSA_EXPORT_WITH_RC4_40_MD5
- RSA_EXPORT_WITH_DES40_CBC_SHA
- RSA_WITH_DES_CBC_SHA
- RSA_WITH_RC4_128_SHA

© 2008 Research In Motion Limited. All rights reserved.

- RSA_WITH_RC4_128_MD5
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- TLS

© 2008 Research In Motion Limited. All rights reserved.

Appendix J: RSA SecurID software token tokencode generation process

1. An administrator uses the RSA Authentication Manager to import the seed in the form of a soft token file in .asc format into the software token database.
2. The administrator uses the RSA Authentication Manager to issue the software token file in .sdtid format. Optionally, the administrator can
   - allow the user to choose whether to set the software token PIN or have the system automatically generate and send a PIN to the user's BlackBerry device, or require the user to set the software token PIN the first time that the user tries to complete two-factor authentication on the BlackBerry device
   - bind the seed to a specific BlackBerry device PIN
   - set a password to encrypt the .sdtid file seed

   Note: Standard BlackBerry encryption is designed to protect the seed when the BlackBerry Enterprise Server sends it over the transport layer.
3. The BlackBerry Enterprise Server administrator sets the .sdtid file seed for the BlackBerry device in the BlackBerry Manager.

   If required, the BlackBerry Enterprise Server administrator types the password to decrypt the seed for use on the BlackBerry device.
4. The BlackBerry Enterprise Server stores the .sdtid file seed in the BlackBerry Configuration Database.
5. The BlackBerry Enterprise Server pushes the .sdtid file seed (and the password, if the administrator set one) to the BlackBerry device during activation of the BlackBerry device and, thereafter, if the administrator changes the .sdtid file seed for the BlackBerry device.

   The BlackBerry device uses RIM-proprietary protocols that are designed to be secure to perform all communication necessary to obtain the seed on behalf of the RSA SecurID Library.
6. The BlackBerry device imports the .sdtid file seed.

   If the administrator set a password in the RSA Authentication Manager to encrypt the .sdtid file seed, the BlackBerry device uses the password to decrypt the .sdtid file seed automatically.

   If the administrator set the .sdtid file seed to bind to a specific BlackBerry device PIN, only that specific BlackBerry device can import the seed successfully.
7. The BlackBerry device stores the .sdtid file seed in flash memory.
8. The BlackBerry device imports a copy of the .sdtid file seed into the RSA SecurID Library on the BlackBerry device.
9. Once each minute, the RSA SecurID library authenticates with the RSA authentication server and initializes the software token algorithm.
10. Each time the BlackBerry device user tries to establish a WLAN or VPN connection that requires two-factor authentication, the BlackBerry device uses the initialized algorithm to combine the .sdtid file seed with random data items based on the BlackBerry device clock and to generate a new software token tokencode.

Appendix K: Content protection initialization process

When the BlackBerry Enterprise Server administrator sets the Content Protection Strength IT policy rule to turn on content protection for a Blackberry device, the following actions occur.

1. The BlackBerry Enterprise Server performs the following actions:
   - picks b randomly
   - calculates $B = bP$
   - stores b in the BlackBerry configuration database
2. The BlackBerry Enterprise Server sends B to the BlackBerry device in the IT policy.

© 2008 Research In Motion Limited. All rights reserved.

3. The BlackBerry device receives B and verifies that *B* is a valid public key.
4. The BlackBerry device performs the following actions:
   - picks *d* randomly
   - calculates *D* = *dP*
   - store *D* in flash memory
   - calculates *K* = *dB*.
5. The BlackBerry device uses *K* to encrypt the current BlackBerry device password, and uses the encrypted password to encrypt the content protection key.
6. The BlackBerry device permanently deletes *d* and *K*.

   When the BlackBerry device permanently deletes *d*, the data that remains stored on the BlackBerry device is not sufficient to recover *K*. Only the BlackBerry Enterprise Server knows *b* and can recalculate *K* = *dB* = *dbP* = *bD* if given *d*.

Appendix L: Protocol for resetting the password on a content-protected BlackBerry device remotely

The protocol for resetting the password on a content-protected BlackBerry device remotely uses elliptic curve cryptography over the NIST recommended 521 bit elliptic curve over a prime field to derive an encryption key from the IT policy public key that the BlackBerry Enterprise Server generates, and use that key to encrypt the content protection key using the encrypted BlackBerry device password. When the BlackBerry Enterprise Server administrator tries to set the BlackBerry device password, the BlackBerry device can rely on the BlackBerry Enterprise Server to provide the data required to reconstruct the derived encryption key. The protocol also uses blinding to prevent the BlackBerry Enterprise Server from reconstructing the derived key itself.

Cryptosystem parameters

The BlackBerry Enterprise Server and the BlackBerry device are designed to share the following cryptosystem parameters when using the protocol for resetting the password on a content-protected BlackBerry device remotely.

Parameter	Description
E(Fq)	the NIST-approved 521-bit random elliptic curve over Fq, which has a cofactor of 1
Fq	a finite field of prime order q
P	a point of E that generates a prime subgroup of E(Fq) of order p
B = *bP*	the long-term IT policy public and private key pair that the BlackBerry Enterprise Server generates for the BlackBerry device; the BlackBerry Enterprise Server stores *b* in the BlackBerry configuration database, and sends *B* to the BlackBerry device in the IT policy
D = *dP*	the key pair that the BlackBerry device creates when it receives *B*; the BlackBerry device stores *D* but deletes *d* to prevent a hardware-based attack from recovering *d* and *B*, and then calculating *K* = *dB*
K = *dB*	the encryption key that the BlackBerry device uses to encrypt the content protection key
r	a short term random number that the BlackBerry device stores in RAM
D' = *rD*	a blinded version of *D*
K' = *bD'* = *brD* = *rK*	a blinded version of *K*

Uppercase letters represent elliptic curve points. Lowercase letters represent scalars. The elliptic curve group operations are additive.

© 2008 Research In Motion Limited. All rights reserved.

Protocol process

When the BlackBerry Enterprise Server administrator sends the Set a Password and Lock Handheld IT administration command to a content-protected BlackBerry device, the following actions occur.

1. The BlackBerry Enterprise Server administrator types the new BlackBerry device password in the BlackBerry Manager.
2. The BlackBerry Enterprise Server sends the Set a Password and Lock Handheld IT administration command and the new BlackBerry device password to the BlackBerry device.
3. The BlackBerry device performs the following actions:
   - picks *r* randomly
   - stores *r* in RAM
   - calculates $D' = rD = rdP$
   - calculates h = SHA-1(B)
4. The BlackBerry device sends D' and h to the BlackBerry Enterprise Server.
5. The BlackBerry Enterprise Server receives D' and h, and performs the following actions:
   - uses h to determine which B the BlackBerry device used, and hence which b to use
   - verifies that D' is a valid public key
   - calculates $K' = bD' = brdP = rdB = rK$ (The BlackBerry Enterprise Server knows only rK, and cannot calculate K without r.)
   - calculates h = SHA-1(D')
6. The BlackBerry Enterprise Server sends the new BlackBerry device password, K', and h to the BlackBerry device.
7. The BlackBerry device receives the new BlackBerry device password, K', and h, and performs the following actions:
   - uses h to verify that K' is associated with D' and r
   - verifies K' is a valid public key
   - calculates $r^{-1}K' = r^{-1}rK = K$
   - permanently deletes r
   - uses K to decrypt the content protection key
   - permanently deletes K
8. The BlackBerry device performs the following actions:
   - picks d randomly
   - calculates $D = dP$
   - store D in flash memory
   - calculates $K = dB$.
9. The BlackBerry device uses K to encrypt the new BlackBerry device password.
10. The BlackBerry device uses the encrypted new password to encrypt the content protection key.

© 2008 Research In Motion Limited. All rights reserved.

Part number: 17930884 Version 2

©2008 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType® and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used as trademarks in the U.S., Canada, and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. Cisco is a trademark of Cisco Systems, Inc. Entrust is a trademark of Entrust, Inc. IBM, Lotus, Domino, and Lotus Notes are trademarks of IBM Corporation. IEEE is a trademark of the Institute of Electrical and Electronics Engineers, Inc. Java is a trademark of Sun Microsystems, Inc. Microsoft, PowerPoint, SQL Server, Outlook, Live Communications Server 2005, and Windows are trademarks of Microsoft Corporation. Netscape is a trademark of Netscape Communication Corporation. Novell and GroupWise are trademarks of Novell, Inc.PGP is a trademark of PGP Corporation. RSA, RSA Security, and SecurID are trademarks of RSA Security. Sun, Java, JSEE, and J2ME are trademarks of Sun Microsystems, Inc. Wi-Fi Protected Access, WPA, and WPA2 are trademarks of the Wi-Fi Alliance. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry smartphone and other devices and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in the U.S. and in various countries around the world. Visit www.rim.com/patents for a list of RIM (as hereinafter defined) patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Research In Motion Limited

295 Phillip Street

Waterloo, ON N2L 3W8

Canada

Research In Motion UK Limited

200 Bath Road

Slough, Berkshire SL1 3XE

United Kingdom

Published in Canada